On m-inverse loops and quasigroups of order n with a long inverse cycle.

by

CARL LOONEY

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

August 2015

To my mother and my father who loved me and have never forsaken me.

ACKNOWLEDGEMENTS

I would like to thank my supervising professor Dr. Minerva Cordero for encouraging me to excel in all my endeavors and also for her invaluable advice during the course of my doctoral studies.

I would also like to thank my father who has always inspired me and has sponsored my career in Mathematics.

<div align="right">July 20, 2015</div>

ABSTRACT

On m-inverse loops and quasigroups of order n with a long inverse cycle.

Carl Looney, Ph.D.

The University of Texas at Arlington, 2015

Supervising Professor: Minerva Cordero

In 2002, A.D Keedwell and V.A Sherbacov introduced the concept of finite m-inverse quasigroups with long inverse cycles. Keedwell and Sherbacov observed that finite m-inverse loops and quasigroups with a long inverse cycle could be useful in the study of cryptology. Keedwell and Sherbacov studied the existence of these algebraic structures by determining if a Cayley table of the elements of such structures could be constructed. They showed that m-inverse loops of order 9 with a long inverse cycle do not exist for m = 2; 4 and 6; thus, there do not exist 2,4, or 6 inverse-quasigroups of order 8. However the investigation of 3 or 7-inverse loops of order 9 and of 3 or 7-inverse quasigroups of order 8 with a long inverse cycle was considered more complicated and was left unanswered. In this paper we attack the unanswered question of the existence of 3 and 7-inverse loops and quasigroups with long inverse cycles. We also investigate the following two problems: (i)The existence of m-inverse loops with a long inverse cycle of orders 11 and 15. (ii)The existence of m-inverse quasigroups with a long inverse cycle of order 12,16 and 20.

TABLE OF CONTENTS

vi

LIST OF TABLES

CHAPTER 1

Introduction

1.1 Introduction

Cryptology is a science that consists of two parts: cryptography and cryptanalysis. Cryptography can be described as the science of transferring information that has been protected from unlawful users[2]. Cryptanalysis is the science of breaking down the transferred information. In general, cryptography requires sets of integers and specific operations that are defined for those sets. The set of elements and the operations that are applied to the elements of the set is called an algebraic structure. Algebraic structures can be classified as associative, such as groups and fields, or non-associative, such as quasigroups and loops. Our focus will be on finite quasigroups and loops. In particular we will study quasigroups with the m-inverse property. We study these particular algebraic structures because Keedwell noticed that finite m-inverse loops and quasigroups with a long inverse cycle were useful in the study of cryptology[1]. In this paper we continue the work of Keedwell where we investigate the existence of finite m-inverse loops and quasigroups with a long inverse cycle. Keedwell's approach for investigating the existence of these algebraic structures was to determine if a Cayley table of the elements can be constructed. The approach consisted of completing row zero in order to determine if a Cayley table exists. In this work, we will continue the same approach for determining the existence of m-inverse loops and quasigroups with a long inverse cycle.

In Chapter 2, we investigate the existence of 3 and 7-inverse loops with a long inverse cycle. We will also investigate the existence of m-inverse quasigroups of order 8 with a long inverse cycle. Next in Chapter 3 we study the existence of finite m-inverse loops with a long inverse cycle where we determine all the possible ways to complete row zero for a finite m-inverse loop. Finally in Chapter 4 we study the existence of finite m-inverse quasigroups with a long inverse cycle where again we determine all the possible ways to complete row zero for a finite m-inverse quasigroup. It is important to note that for finite m-inverse loops and quasigroups with a long inverse cycle we examine all the possible ways to complete row zero. This is important because one of these forms may lead to the construction of a Cayley table. However if all ways to complete row zero fail to construct a Cayley table then we conclude that a finite m-inverse loop or quasigroup with a long inverse cycle does not exist.

Definition 1.1

A finite *quasigroup* $(Q, *)$ of order n consists of a set Q of n symbols on which a binary operation $(*)$ is defined such that for all $a, b \in Q$, $a * b \in Q$, and there exist unique $x, y \in Q$ such that $x * a = b$ and $a * y = b$. If there exists an identity element $e \in Q$ such that for all $a \in Q$, $a * e = e * a = a$ then $(Q, *)$ is a *loop*.

Definition 2.1

The **Cayley table** of a finite quasigroup is a table with rows and columns labelled by the elements of the group and the entry $a * b$ in the row labelled by a and column labelled by c.

Here is an example of the Cayley table of quasigroup $(Z_3, +)$. Notice that we will call "row a" the row giving the products $a * x$ for all $x \in Q$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Definition 3.1

Let $(Q, *)$ be a *quasigroup* (respectively a *loop*). Then $(Q, *)$ is an m-inverse quasigroup/loop if there exists a permutation J of the set Q such that for all $a, b \in Q$, $J^m(a * b) * J^{m+1}(a) = J^m(b)$.

If $(Q, *)$ is a quasigroup/loop then $Q = \{e, 0, 1.....n - 2\}$ or $\{0, 1.....n - 1\}$ respectively. Note for our study of m-inverse loops and quasigroups we will define J as $J(a) \equiv a + 1$, where the arithmetic is modulo $n - 1$ when discussing loops and modulo n for quasigroups.

CHAPTER 2

3 and 7-inverse loops and quasigroups

2.1   3 and 7-inverse loops of order 9 with a long inverse cycle

In this chapter we determine the existence of 3 and 7-inverse loops of order 9 with a long inverse cycle. We also determine if 3 and 7-inverse quasigroups of order 8 with a long inverse cycle exist. Determining the existence of a m-inverse loop of order 9 and a m-inverse quasigroup of order 8 with a long inverse cycle was the stopping point for Keedwell in his paper written on m-inverse loops and quasigroups[1]. Now in order to determine if a m-inverse loop or quasigroup with a long inverse cycle exists we follow Keedwell's approach and determine if a Cayley table of the set Q can be constructed. If all attempts to construct a Cayley table fail then we conclude that a 3 or 7-inverse loop of order 9 and a 3 or 7-inverse quasigroup of order 8 does not exist. Note that for 3 and 7 inverse loops and quasigroups with a long inverse cycle the arithmetic is modulo 8.

2.1.1   3-inverse loops of order 9 with a long inverse cycle

Suppose that $(Q, *)$ is a 3-inverse loop of order 9 with a long inverse cycle and $a * b = c$ where $a, b, c \in Q$. Therefore, by the m-inverse property a permutation J exists such that $[J^3(a * b)] * [J^4(a)] = J^3(b)$ for all $a, b \in Q$. Let $J(a) \equiv a + 1$; then $J(J(a)) = J(a + 1) \equiv a + 2$. Therefore by applying J, $m - 1$ times we obtain $J^m(a) \equiv a + m$. Consider $[J^m(a * e)] * [J^{m+1}(a)] = J^m(e)$ for $a \in Q$. This implies that $[J^m(a)] * [J(J^m(a)] = e$. Let $J^m(a) = b \in Q$. It follows that $b * J(b) = e = b * (b + 1)$.

Let $a * b = c$. Thus $[J^3(c)] * [J^4(a)] = J^3(b)$ which implies that $(c+3) * (a+4) = (b+3)$. From the equality $(c+3) * (a+4) = (b+3)$ we obtain $[J^3(b+3)] * [J^4(c+3)] = J^3(a+4)$ which implies that $(b+6) * (c+7) = (a+7)$. Next from the equality $(b+6) * (c+7) = (a+7)$ we obtain $[J^3(a+7)] * [J^4(b+6)] = J^3(c+7)$ which implies that $(a+2) * (b+2) = c+2$. Therefore, if $a * b = c$, then $(c+3) * (a+4) = (b+3)$, $(b+6) * (c+7) = (a+7)$ and $(a+2) * (b+2) = c+2$.

Next we describe how to obtain the equalities for a 3-inverse loop of order 9 in general for the choice $a * b = c$. First we add 3 to the last term in the previous equality to obtain the first term in the new equality. Next we add 4 to the first term in the previous equality to obtain the second term in the new equality. Lastly, we add 3 to the second term in the previous equality to obtain the last term in the new equality. This process will continue until we reach $[a + s(3m+1)] * [b + s(3m+1)] = c + s(3m+1)$ where s is the smallest positive integer such that $s(3m+1) \equiv 0$. Therefore, by letting $a * b = c$ the set of equalities given in Table 2.1 hold. We will say that the choice $a * b = c$ generates each equality.

Table 2.1. Iteration 2.1

$a * b = c$
$(c + 3) * (a + 4) = (b + 3)$
$(b + 6) * (c + 7) = (a + 7)$
$(a + 2) * (b + 2) = (c + 2)$
$(c + 5) * (a + 6) = (b + 5)$
$b * (c + 1) = (a + 1)$
$(a + 4) * (b + 4) = (c + 4)$
$(c + 7) * a = (b + 7)$
$(b + 2) * (c + 3) = (a + 3)$
$(a + 6) * (b + 6) = (c + 6)$
$(c + 1) * (a + 2) = (b + 1)$
$(b + 4) * (c + 5) = (a + 5)$

The elements of Q are $e, 0, 1....7$. This implies the given entries for the Cayley table are: $0*1 = e$, $1*2 = e$, ..., $7*0 = e$ and $0*e = 0 = e*0 = 0$,......, $7*e = 7 = e*7$. Therefore, we are given 25 entries of the Cayley table associated with Q. Thus 56 entries have yet to be inputted into the Cayley table. Recall that "row a" is the row yielding the product $a*x$ for all $x \in Q$. Consider the missing entries in row zero: $0*0$, $0*2$, $0*3$, $0*4$, $0*5$, $0*6$ and $0*7$. Next we fill row zero in the following way: Let $0*0 = 3$, $0*2 = 4$, $0*3 = 7$, $0*4 = 1$, $0*5 = 3$, $0*6 = 5$ and $0*7 = 6$. Therefore, since we assumed $(Q, *)$ is a 3-inverse loop of order 9 we obtain the following partially completed Cayley table.

*	e	0	1	2	3	4	5	6	7
e	e	0	1	2	3	4	5	6	7
0	0	3	e	4	7	1	2	5	6
1	1	4	3	e	?	2	?	7	5
2	2	7	0	5	e	6	1	3	4
3	3	1	7	6	5	e	?	4	?
4	4	5	6	1	2	7	e	0	3
5	5	6	?	3	1	0	7	e	?
6	6	2	5	7	0	3	4	1	e
7	7	e	?	0	?	5	3	2	1

Consider row one since the entries 0 and 6 are missing from row one then $1*3 = 0$ or $1*3 = 6$. Therefore we obtain the following iterations:

Table 2.2. Iteration 2.2

$1*3 = 0$	$1*3 = 6$
$3*5 = 6$	$1*5 = 6$
$1*7 = 0)$	

Notice that each choice leads to a contradiction. Therefore, by completing row zero in this manner we are not able to construct a Cayley table. Now if we continue to construct the partial Cayley table by checking all the possible choices for the missing entries in row zero then we will have numerous cases: Therefore, to eliminate this tedious process we introduce the following lemma and propositions that we help us generalize the construction of row zero.

Lemma 1. *If $(Q, *)$ is a 3-inverse loop of order 9 with a long inverse cycle then the choice $a * b = c$ generates 12 or 4 entries in the Cayley table.*

Proof. Notice that from table 2.1 it is clear that the choice $a * b = c$ generates at most 12 distinct entries in the Cayley table. Let's assume that $a * b = c$ generates $t < 12$ entries in the Cayley table. This implies that t divides 12. Therefore, $t = 1, 2, 3, 4$ or 6. If $a * b = c$ generates 3 or 6 entries then by table 2.1 $a \equiv a + 2$ or $a \equiv a + 6$, respectively, which is a contradiction since the arithmetic is modulo 8. Assume $t = 1$ or 2; by table 2.1 $a \equiv a + 2$ or $a \equiv a + 4$ respectively, which again is a contradiction since the arithmetic is modulo 8. Finally if $t = 4$, then $b \equiv a + 6$ and $c \equiv a + 3$ where $a * (a + 6) = a + 3$ generates 4 entries in the Cayley table. $\square$

In the next proposition we study the product $0 * b = c$ for $b, c \in Q$ and consider the entries the product generates in row zero depending on whether they are even or odd.

Proposition 1. *Let $(Q, *)$ be a 3-inverse loop of order 9 with a long inverse cycle.*

1. If $0 * b = c$ generates 12 distinct entries in the Cayley table with b even and c odd then the choice $0 * b = c$ generates 3 odd entries in row zero.

7

2. If $0 * b = c$ generates 12 distinct entries in the Cayley table such that b and c are even then the choice $0 * b = c$ generates one odd and one even entry in row zero.

3. If $0 * b = c$ generates 12 distinct entries in the Cayley table with b odd and c even then the choice $0 * b = c$ generates one even entry in row zero.

Proof. 1. Assume $0 * b = c$ generates 12 distinct entries in row zero with b even and c odd. Consider table 2.1. Notice that the first term in each equation is in the form $a + x_i$, $c + y_i$ or $b + z_i$ for $i = 1, .., 4$ and $x_i, y_i, z_i \in Q$. Each term respectively determines what row the entry will be inputted in. We know that $a = 0$, b is even and c is odd. Therefore, each term is congruent to some even element of Q. Thus for some i each term is congruent to zero where the entries are odd.

2. Assume $0 * b = c$ generates 12 distinct entries in row zero such that b and c are even. Consider table 2.1. Again the first term in each equation is in the form $a + x_i$, $c + y_i$ or $b + z_i$ for $i = 1, .., 4$ where $x_i, y_i, z_i \in Q$. Each term respectively determines what row the entry will be inputted in. We know that $a = 0$, b and c are even. Therefore, only $a + x_i$ and $b + z_i$ are congruent to some even element of Q. Thus for some i each term is congruent to zero where the entry associated with $a + x_i$ is even and the entry associated with $b + z_i$ is odd.

3. Assume $0 * b = c$ generates 12 distinct entries in row zero with b odd and c even. Consider table 2.1. Again the first term in each equation is in the form $a + x_i$, $c + y_i$ or $b + z_i$ for $i = 1, .., 4$ and $x_i, y_i, z_i \in Q$. Each term respectively determines what row the entry will be inputted in. We know that $a = 0$, b is odd and c is even. Therefore, only $a + x_i$ is congruent to some even element of Q. Thus, for some i, $a + x_i$, is congruent to zero where the entry associated with $a + x_i$ is even.

$\square$

Proposition 2. *If $(Q, *)$ is a 3-inverse loop of order 9 with a long inverse cycle such that $0 * 6 = 3$ then the choice $0 * 6 = 3$ generates 4 distinct entries in the Cayley Table.*

Proposition 3. *Let $(Q, *)$ be a 3-inverse loop of order 9 with a long inverse cycle and let the choice $0 * b = c$ generate 3 odd entries in row zero. Then $0 * 6 \neq 3$.*

Proof. By computing the possible choices that generates 3 entries in row zero we obtain that if the choice $0*b = c$ generates 3 entries in the Cayley table then $0*6 = 5$.

$\square$

Let A be the set of all the equalities $0 * b = c$ that generate 3 odd entries in row zero. Let B be the set of all the equalities $0 * b = c$ that generate one even and one odd entry in row zero. Finally let C be the set of all the equalities $0 * b = c$ that generate one even entry in row zero. Recall that the choice $a * b = c$ generates 12 or 4 entries in the Cayley table. If $a * b = c$ generates 4 entries in the Cayley table then $a * (a + 6) = a + 3$. Hence $0 * 6 = 3$ and $1 * 7 = 4$. Thus to obtain the 56 missing entries we need a combination of equalities that generate 12 distinct entries in the Cayley table for the following reasons. We know that there can only be two choices that generate 4 entries in the Cayley table. This implies that the remaining choices $a * b = c$ must generate 12 distinct entries in the Cayley table. Therefore in order to obtain the 56 missing entries we must find $y \leq 2 \ x, y \in Z^+$ that satisfy the following equation $12x + 4y = 56$. This implies that $x = 4$ and $y = 2$. Therefore, in order for a m-inverse loop of order 9 to exist we need the choice $0 * 6 = 3$, the choice $1 * 7 = 4$ and four equalities that generate 12 distinct entries each in the Cayley table.

Notice that from row zero we have the choices $0 * e = 0$, $0 * 1 = e$ and $0 * 6 = 3$. Therefore, there are three odd and three even entries missing in row zero. Furthermore

by proposition 3, if we choose $0*b = c \in A$ then $0*6 \neq 3$. However, $0*6 = 3$. Therefore the remaining odd entries in row zero must be obtained by some combination of $0 * b = c \in B$. Recall that each $0 * b = c \in B$ generates one odd and one even entry in row zero. Therefore, we need three equalities from set B in order to complete row zero.

Next we determine if the completion of row zero leads to the construction of a Cayley Table. We have three choices $0*b = c$ from B that generate 12 distinct entries in the Cayley table, and the choices $0 * 6 = 3$ and $1 * 7 = 4$ that generate 4 entries in the Cayley table, respectively. Therefore we have a total of 44 of 56 missing entries. Now the choice $a * b = c$ generates 12 or 4 entries in the table. Therefore we need some $a * b = c$ that generates 12 distinct entries in the Cayley table after row zero is filled. Recall that the choice $0 * b = c \in B$ generates one odd entry in row one. This implies that by completing row zero we obtain three odd entries in row one and one even entry in row one since $1 * 7 = 4$. By letting $(Q, *)$ be a m-inverse loop of order 9 we obtain $1*e = 1$, $1*2 = e$, $1*7 = 4$. Therefore $0, 2, 6$ are the missing entries in row one after row zero is completed. This implies that there exist some choice $1 * b = c$ that generates the entries $0, 2, 6$ in row one after row zero is completed. We assume that some $1 * b = c$ generates 12 distinct entries in the Cayley table and row zero is filled. The table below will assist us in determining if the elements $b \in Q$ and $c \in Q$ are odd or even. It is important to note that the first term in each equality determines the row and the second term determines the column the entry will be inputted in.

Table 2.3. Iteration 2.3

$1 * b = c$
$(c+3) * 5 = (b+3)$
$(b+6) * (c+7) = 0$
$3 * (b+2) = (c+2)$
$(c+5) * 7 = (b+5)$
$b * (c+1) = 2$
$5 * (b+4) = (c+4)$
$(c+7) * 1 = (b+7)$
$(b+2) * (c+3) = 4$
$7 * (b+6) = (c+6)$
$(c+1) * 3 = (b+1)$
$(b+4) * (c+5) = 6$

Consider the first term in each equation in table 2.2. Notice that the first terms for the set of equations are: $1, 3, 5, 7$, $c + x_i$ and $b + y_i$ with x_i odd and y_i even for $i = 1, .., 4$. Thus c is congruent to some even element of Q and b is congruent to some odd element of Q. Hence the choices for b are $1, 3, 5$ and the choices for c are $0, 2, 6$. Consider the following table:

Table 2.4. Iteration 2.4

$1*1=0$	$1*1=6$	$1*3=0$	$1*3=2$	$1*3=6$	$1*5=0$	$1*5=2$
$3*5=4$	$1*5=4$	$3*5=6$	$5*5=6$	$1*5=6$	$3*5=0$	$5*5=0$
$7*7=0$		$1*7=0$	$1*1=0$			$3*1=0$
$3*3=2$						$3*7=4$
$5*7=6$						$7*7=2$
$1*1=2$						$5*3=2$
						$5*1=6$
						$1*1=4$

11

Notice that from column 1 of table 2.3, $1 * 1 = 0$ and $1 * 1 = 2$. However if $1 * 1 = 0$ then $1 * 1 \neq 2$ since $0 \not\equiv 2$. Therefore $1 * 1 \neq 0$ or $1 * 1 \neq 2$. Now considering column 2, we conclude that if $1 * 1 = 6$ then $1 * 5 = 4$. However, $1 * 7 = 4$. Thus $1 * 1 \neq 6$. This implies that $1 * 1 \neq 0$, $1 * 1 \neq 6$ or $1 * 1 \neq 2$. By examining each individual column we obtain that these choices for $1 * 1, 1 * 3$ and $1 * 5$ cannot equal $0, 2$ or 6. This implies that there does not exist a choice $1 * b = c$ that generates the entries $0, 2, 6$ in row one after row zero is filled. Therefore, we are not able to construct a Cayley table associated with Q. Thus we conclude a 3-inverse loop of order 9 with a long inverse cycle does not exist.

2.1.2   7-inverse loop of order 9 with a long inverse cycle

In this section we investigate the existence of a 7-inverse loop of order 9. First we observe the following iterations:

Table 2.5. Iteration 2.5

$m = 3$	$m = 7$
$a * b = c$	$a * b = c$
$(c + 3) * (a + 4) = (b + 3)$	$(c + 7) * a = (b + 7)$
$(b + 6) * (c + 7) = (a + 7)$	$(b + 6) * (c + 7) = (a + 7)$
$(a + 2) * (b + 2) = (c + 2)$	$(a + 6) * (b + 6) = (c + 6)$
$(c + 5) * (a + 6) = (b + 5)$	$(c + 5) * (a + 6) = (b + 5)$
$b * (c + 1) = (a + 1)$	$(b + 4) * (c + 5) = (a + 5)$
$(a + 4) * (b + 4) = (c + 4)$	$(a + 4) * (b + 4) = (c + 4)$
$(c + 7) * a = (b + 7)$	$(c + 3) * (a + 4) = (b + 3)$
$(b + 2) * (c + 3) = (a + 3)$	$(b + 2) * (c + 3) = (a + 3)$
$(a + 6) * (b + 6) = (c + 6)$	$(a + 2) * (b + 2) = (c + 2)$
$(c + 1) * (a + 2) = (b + 1)$	$(c + 1) * (a + 2) = (b + 1)$
$(b + 4) * (c + 5) = (a + 5)$	$b * (c + 1) = (a + 1)$
$a * b = c$	$a * b = c$

From the above iterations, we observe that for $m = 3$ and $m = 7$ the choice $a * b = c$ generates the same equalities. Therefore, if $m = 7$ we obtain the same results as when $m = 3$. Thus we conclude that a 7-inverse loop of order 9 with a long inverse cycle does not exist. We have proven the following theorem.

Theorem 1. *A 3 or 7-inverse loop of order 9 with a long inverse cycle does not exist.*

2.1.3   3-inverse quasigroups of order 8 with a long inverse cycle

The objective of this section is to determine if there exists a 3-inverse Quasigroup of order 8 with a long inverse cycle. Let's assume a 3-inverse quasigroup of order 8 with a long inverse cycle exists and let $Q = \{e, 0, 1, ..., 7\}$. This implies that there exists a permutation J such that $[J^3(a * b)] * [J^4(a)] = J^3(b)$ for all $a, b \in Q$ where $J(a) \equiv a + 1$. Therefore we obtain the following equalities.

Table 2.6. Iteration 2.6

$a * b = c$
$(c + 3) * (a + 4) = (b + 3)$
$(b + 6) * (c + 7) = (a + 7)$
$(a + 2) * (b + 2) = (c + 2)$
$(c + 5) * (a + 6) = (b + 5)$
$b * (c + 1) = (a + 1)$
$(a + 4) * (b + 4) = (c + 4)$
$(c + 7) * a = (b + 7)$
$(b + 2) * (c + 3) = (a + 3)$
$(a + 6) * (b + 6) = (c + 6)$
$(c + 1) * (a + 2) = (b + 1)$
$(b + 4) * (c + 5) = (a + 5)$

Notice that the equalities are the same as when investigating 3 and 7-loops of order 9 with a long inverse cycle. We obtain similar results for quasigroup and the proofs are the same as the corresponding ones for loops.

Lemma 2. *If $(Q, *)$ is a 3-inverse quasigroup of order 8 with a long inverse cycle then the choice $a * b = c$ generates 12 or 4 entries in the Cayley table.*

Proposition 4. *Let $(Q, *)$ be a 3-inverse quasigroup of order 8 with a long inverse cycle.*

1. If $0 * b = c$ generates 12 distinct entries in the Cayley table with b even and c odd then the choice $0 * b = c$ generates 3 odd entries in row zero.

2. If $0 * b = c$ generates 12 distinct entries in the Cayley table such that b and c are even then the choice $0 * b = c$ generates one odd and one even entry in row zero.

3. If $0 * b = c$ generates 12 distinct entries in the Cayley table with b odd and c even then the choice $0 * b = c$ generates one even entry in row zero.

Proposition 5. *Let $(Q, *)$ be a 3-inverse quasigroup of order 8 with a long inverse cycle such that the choice $0 * 6 = 3$. Then the choice $0 * 6 = 3$ generates 4 distinct entries in the Cayley table.*

Proposition 6. *If $(Q, *)$ is a 3-inverse quasigroup of order 8 with a long inverse cycle and the choice $0 * b = c$ generates 3 odd entries in row zero then $0 * 6 \neq 3$.*

Proposition 7. *Let $(Q, *)$ be a 3-inverse quasigroup of order 8 with a long inverse cycle and the choice $a * b = c$ generates 4 entries in the Cayley table. Then $a * b = c$ generates $0 * 6 = 3$ or $1 * 7 = 4$.*

Let the definition for A,B and C hold as previously stated when investigating m-inverse loops of order 9. Let $(Q, *)$ be a 3-inverse quasigroup of order 8 with a long inverse cycle. This implies that there are 64 missing entries in the Cayley table. We know that there can only be two choices that generate 4 distinct entries in the Cayley table. This implies that the remaining choices $a * b = c$ must generate 12 distinct entries in the Cayley table. Therefore in order to obtain the 64 missing entries we must find $x, y \in Z^+$ that satisfy the equation $12x + 4y = 64$, where x represents the number of equalities that generate 12 distinct entries in the Cayley table, and y represents the number of equalities that generate 4 entries in the Cayley table and $y \leq 2$. This implies that $x = 5$ and $y = 1$. Therefore, in order for a m-inverse quasigroup of order 8 to exist we need four equalities that generate 12 distinct entries each in the Cayley table corresponding to the choice $0 * 6 = 3$, or the choice $1 * 7 = 4$. Let $0 * 6 = 3$; this implies that $0 * b = c \notin A$. Therefore we need three equalities from B that generate the remaining odd missing entries in row zero. This combination yields three odds and three even entries in row zero. This implies that there remains one even entry missing in row zero. Therefore, we need one equality $0 * b = c \in C$ to complete row zero. Let $0 * 0 = 2 \in B$, $0 * 2 = 0 \in B$, $0 * 4 = 4 \in B$, $0 * 5 = 6 \in C$, $0 * 6 = 3$, and $1 * 1 = 4$. Notice that the choices $0 * 6 = 3$ and $1 * 1 = 4$ are not contained in the set A, B or C. The choice $0 * 6 = 3$ generates 4 entries in the Cayley table and the choice $1 * 1 = 4$ generates no entries in row zero. It is important to note that a set has not been defined for these choices. We obtain the following Cayley

table which implies that a 3-inverse quasigroup of order 8 with a long inverse cycle does exist.

Table 2.7. 3-inverse quasigroup of order 8 with a long inverse cycle

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

Here is an example of a 3-inverse quasigroup of order 8 with a long inverse cycle where $1 * 7 = 4$ but $0 * 6 \neq 3$.

Table 2.8. 3-inverse quasigroup of order 8 with a long inverse cycle

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

2.1.4   7-inverse quasigroups of order 8 with a long inverse cycle

In this section we investigate the existence of a 7-inverse quasigroup of order 8 with a long inverse cycle. Let's observe the iteration listed below.

Table 2.9. Iteration 2.9

$m = 3$	$m = 7$
$a * b = c$	$a * b = c$
$(c + 3) * (a + 4) = (b + 3)$	$(c + 7) * a = (b + 7)$
$(b + 6) * (c + 7) = (a + 7)$	$(b + 6) * (c + 7) = (a + 7)$
$(a + 2) * (b + 2) = (c + 2)$	$(a + 6) * (b + 6) = (c + 6)$
$(c + 5) * (a + 6) = (b + 5)$	$(c + 5) * (a + 6) = (b + 5)$
$b * (c + 1) = (a + 1)$	$(b + 4) * (c + 5) = (a + 5)$
$(a + 4) * (b + 4) = (c + 4)$	$(a + 4) * (b + 4) = (c + 4)$
$(c + 7) * a = (b + 7)$	$(c + 3) * (a + 4) = (b + 3)$
$(b + 2) * (c + 3) = (a + 3)$	$(b + 2) * (c + 3) = (a + 3)$
$(a + 6) * (b + 6) = (c + 6)$	$(a + 2) * (b + 2) = (c + 2)$
$(c + 1) * (a + 2) = (b + 1)$	$(c + 1) * (a + 2) = (b + 1)$
$(b + 4) * (c + 5) = (a + 5)$	$b * (c + 1) = (a + 1)$
$a * b = c$	$a * b = c$

From the above iteration notice that if $(Q, *)$ is a m-inverse quasigroup of order 8 with a long inverse cycle then for $m = 3$ or $m = 7$ the choice $a * b = c$ generates the same entries for the Cayley table. Therefore, since there exist a 3-inverse quasigroup

of order 8 with a long inverse cycle, then there also exist a 7-inverse quasigroup of order 8 with a long inverse cycle. Here is an example when $0 * 6 = 3$.

Table 2.10. 7-inverse quasigroup of order 8 with a long inverse cycle.

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

Next we give an example when $1 * 7 = 4$.

Table 2.11. 7-inverse quasigroup of order 8 with a long inverse cycle

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

We have proven the following theorem.

Theorem 2. *A 3 and 7-inverse quasigroup of order 8 with a long inverse cycle exists.*

18

CHAPTER 3

The existence of m-inverse loops of order n with a long inverse cycle

3.1 Introduction to m-inverse loops with a long inverse cycle

In this chapter we generalize our results by investigating the existence of m-inverse loops of order $3k$ and $3k + 2$ with a long inverse cycle. The following theorem was proven by Keedwell in his paper on m-inverse loops and quasigroups.[1]

Theorem 3. *A m-inverse loopof order n=3k+1 with an inverse cycle of length 3k does not exist for $k \in Z^+$.*

Since we know that these structures do not exist for orders 3k+1 we are left to investigate the orders 3k and 3k+2. We may suppose without lost of generality that the elements of Q are $e, 0, 1.......n - 2$ where e is the identity element, and that the notation is chosen so that $J = (e)(0, 1.....n - 2)$: that is, so that $(0, 1.....n - 2)$ is the long inverse cycle and $J(a) \equiv a + 1 \ mod(n - 1)$. Recall for a m-inverse loop $a * J(a) = e$ for all $a \in Q$. Therefore $a * (a + 1) = e$. When investigating the existence of these algebraic structures we will examine the possible entries for a Cayley table to determine if the choice $a * b = c$ leads to the construction of a Cayley table. If we are able to construct a Cayley table of the elements of $(Q, *)$ where J is a permutation of Q such that $[J^m(a * b)] * [J^{m+1}(a)] = J^m(b)$ then a m-inverse loop exists.

We begin the investigation in the same manner as when we investigated m-inverse loops of order 9 with a long inverse cycle. We assume that $(Q, *)$ is a m-inverse loop of order n with a long inverse cycle. Next we determine all the possible ways that row zero can be constructed. Recall, when we were investigating the

existence of m-inverse loops of order 9, after row zero was completed we obtained a partially completed Cayley table. We only needed to complete the remaining missing entries in row 1 to determine the existence of the algebraic structure. Therefore, by completing row zero the majority of the work was done. Thus for m-inverse loops of order $3k$ and $3k + 2$ we will assume that after row zero is complete we will have a partially completed Cayley table. If the structure exists the Cayley table then can be constructed by completing row one. Therefore, our main focus will be on completing row zero and row one.

It is important to note that we will only investigate m-inverse loops with a long inverse cycle that meet the following conditions: First m, and n are odd; therefore $gcd(3m + 1, n - 1) > 1$. Secondly, $(n - 1)/2$ is the smallest positive integer such that $[(n - 1)/2](3m + 1) \equiv 0 \ mod(n - 1)$, where $3m + 1 \equiv a \ mod(n - 1)$ for $a \in Q$. Therefore, $x(3m + 1) \equiv b \ mod(n - 1)$ for $b \in Q$ for some $x \in Z^+$. Recall that we are assuming that after row zero is filled we have a partially complete table. Therefore, the choice $a * b = c$ generates the entry c and some other entries in the Cayley table not necessarily in row a, as we now describe. Recall by definition of a m-inverse loop of order n with a long inverse cycle, that there exist a permutation J such that $[J^m(a * b)] * [J^{m+1}(a)] = [J^m(b)]$ and $J(a) \equiv a + 1 \ mod(n - 1)$. Notice that since $J(a) \equiv a + 1 \ mod(n - 1)$ then $J(J(a)) = J(a + 1) \equiv a + 2 \ mod(n - 1)$. Therefore if we apply J m times then $J^m(a) \equiv a + m \ mod(n - 1)$. Therefore, from the choice $a * b = c$ we derive the following: $[J^m(c)] * [J^{m+1}(a)] = [J^m(b)]$ which implies that $[(c + m)] * [a + (m + 1)] = [(b + m)]$. Then from the equality $[(c+m)]*[a+(m+1)] = [(b+m)]$ we obtain $[J^m(b+m)]*[J^{m+1}(c+m)] = [J^m(a+(m+1)]$ which implies that $[(b + 2m)] * [c + (2m + 1)] = [a + (2m + 1)]$. Next from the equality $[(b+2m)]*[c+(2m+1)] = a+(2m+1)]$ we obtain $[J^m(a+(2m+1))]*[J^{m+1}(b+2m)] =$

20

$[J^m(c+(2m+1))]$ which implies that $[a+(3m+1)]*[b+(3m+1)] = [c+(3m+1)]$.

Therefore, from the choice $a*b = c$ we obtain $[(c+m)]*[a+(m+1)] = [(b+m)]$,

$[(b+2m)]*[c+(2m+1)] = [a+(2m+1)]$ and $[a+(3m+1)]*[b+(3m+1)] = [c+(3m+1)]$.

Notice that if we choose $a*b = c$ then in order to obtain the next equality we add m to

c so that we get the first term in the new equality. Next we add $m+1$ to a to get the

second term in the new equality. Then finally we add m to b to obtain the last term in

the new equality. Therefore, to determine how to obtain the equalities generated by

the choice $a*b = c$ in general we will add m to the last term in the previous equality

to obtain the first term in the new equality. Next we add $m+1$ to the first term in the

previous equality to obtain the second term in the new equality. And finally we add m

to the second term in the previous equality to obtain the last term in the new equality.

This process will continue until we reach $[a+s(3m+1)]*[b+s(3m+1)] = [c+s(3m+1)]$

where s is the smallest positive integer such that $s(3m+1) \equiv 0 \ mod(n-1)$ since Q

is finite. Therefore, if $a*b = c$ then the set of equalities given below must hold; we

say that the choice $a*b = c$ generates each equality in the set. Let $x = s-1$.

Table 3.1. Iteration 3.1

$a*b = c$
$[c+m]*[a+(m+1)] = [b+m]$
$[b+2m]*[c+(2m+1)] = [a+(2m+1)]$
$[a+1(3m+1)]*[b+1(3m+1)] = [c+1(3m+1)])$
$[c+1(3m+1)+m]*[a+1(3m+1)+(m+1] = [b+1(3m+1)+m]$
$[b+1(3m+1+2m]*[c+1(3m+1)+(2m+1)] = [a+1(3m+1)+(2m+1)]$
$[a+2(3m+1)]*[b+2(3m+1)] = [c+2(3m+1)]$
$[c+2(3m+1)+m]*[a+2(3m+1)+(m+1] = [b+2(3m+1)+m]$
$[b+2(3m+1)+2m]*[c+2(3m+1)+(2m+1] = [a+2(3m+1)+(2m+1)]$
....

....
$[a+x(3m+1)]*[b+x(3m+1)] = [c+x(3m+1)]$
$[c+x(3m+1)+m]*[a+x(3m+1)+(m+1)] = [b+x(3m+1)+m]$
$[b+x(3m+1)+2m]*[c+x(3m+1)+(2m+1)] = [a+x(3m+1)+(2m+1)]$
$[a+s(3m+1)]*[b+s(3m+1)] = [c+s(3m+1)]$

It is important to reiterate that we will only study m-inverse loops where $s = (n-1)/2$. Recall that the arithmetic for m-inverse loops of order n is modulo n-1, the arithmetic for m-inverse quasigroups of order n is modulo n. Notice that the equations in table 3.1 can be represented by the equations in table 3.2 listed below. We will refer to table 3.2 as X_j for $j = 0, 1, ...s-1$.

Table 3.2. Iteration 3.2

$$[a + j(3m+1)] * [b + j(3m+1)] = [c + j(3m+1)]$$
$$[c + j(3m+1) + m] * [a + j(3m+1) + (m+1)] = [b + j(3m+1) + m]$$
$$[b + j(3m+1) + 2m] * [c + j(3m+1) + (2m+1)] = [a + j(3m+1) + (2m+1)]$$

Since $j = 0, 1, ...s-1$, there exist a maximum of $3s$ equalities that hold. Note that if the choice $a * b = c$ generates t entries in the Cayley table and $t \neq 3s$ then t divides $3s$. Also when discussing or deriving any results related to the entries in the Cayley table we will only need to refer to the set X_j for $j = 0, 1, ...s-1$ since the equalities of this set yield the entries in the Cayley table. Next we investigate each equality in X_j to derive an equivalent form. This form will assist us in determining the value of t when the choice $a * b = c$ generates $t < 3s$ entries in the Cayley table.

Now observe the following table in which we rewrite the terms that are added to a, b and c in the set X_j.

Table 3.3. Iteration 3.3

$j(3m + 1) = (3j)m + j$
$j(3m + 1) + m = (3(j + 1))m + j$
$j(3m + 1) + m + 1 = (3j + 1))m + (j + 1)$
$j(3m + 1) + 2m = (3j + 2)m + j$
$j(3m + 1) + 2m + 1 = (3j + 2)m + (j + 1)$

Let $j - 1 = x_0$ Using this table we rewrite the equalities generated by the choice $a * b = c$ in the following way.

Table 3.4. Iteration 3.4

$a * b = c$
$[c + m] * [a + (m + 1)] = [b + m]$
$[b + 2m] * [c + (2m + 1)] = [a + (2m + 1)]$
$[a + (3m) + 1] * [b + (3m) + 1][= c + 1(3m) + 1]$
$[c + (4m) + 1] * [a + (4m) + 2)] = [b + (4m) + 1]$
$[b + (5m) + 1] * [c + (5m) + 2] = [a + (5m) + 2]$
$[a + (6m) + 2] * [b + (6m) + 2] = [c + (6m) + 2]$
$[c + (7m) + 2] * [a + (7m) + 3] = [b + (7m) + 2]$
$[b + (8m) + 2] * [c + (8m) + 3)] = [a + (8m) + 3]$
....
....
$[a + 3(x_0)m + (x_0)] * [b + (3(x_0)m + (x_0)] = [c + 3(x_0)m + (x_0)]$
$[c + (3(x_0) + 1)m + (x_0)] * [a + (3(x_0) + 1)m + (x_0) + 1] = [b + (3(x_0) + 1)m + (x_0)]$
$[b + (3(x_0) + 2)m + (x_0)] * [c + (3(x_0) + 2)m + (x_0) + 1] = [a + (3(x_0) + 2)m + (x_0) + 1]$
$[a + j(3m+)] * [b + j(3m + 1) = c + j(3m + 1)]$

Assume that the choice $a * b = c$ generates 3 entries in the Cayley table. This implies that $a * b = c, (c + m) * [a + (m + 1)] = (b + m)$ and $(b + 2m) * [c + (2m + 1)] = [a + (2m + 1)]$. Now in order to determine how many entries the choice $a * b = c$ generates in the Cayley table we start with the choice $a * b = c$ and keep adding m and $m + 1$ to the appropriate terms until we obtain the choice $a * b = c$ for a second time. Then we determine how many equalities hold before the choice $a*b = c$ appears

a second time; that number will be the amount of entries the choice $a * b = c$ has generated. This implies that if $a * b = c$ generates 3 entries in the Cayley table, the choice $a * b = c$ is equivalent to $[a + (3m + 1)] * [b + (3m + 1)] = [c + 1(3m + 1)]$. Thus $a \equiv a + (3m + 1)$ $b \equiv b + (3m + 1)$ and $c \equiv c + (3m + 1)$. Next let the choice $a * b = c$ generate 4 entries in the Cayley table. This implies that the choice $a * b = c$ is equivalent to $[c + (4m + 1 + m)] * [a + (4m + 2))] = [b + (4m + 1)]$. Thus $a \equiv c + (4m) + 1$, $b \equiv a + (4m + 2)$ and $c \equiv b + (4m) + 1$. Next let the choice $a * b = c$ generate 5 entries in the Cayley table. This implies that the choice $a * b = c$ is equivalent to $[b + (5m + 1)] * [c + (5m + 2)] = [a + (5m + 2)]$. Therefore $a \equiv b + (5m + 1)$, $b \equiv c + (5m + 2)$ and $c \equiv a + (5m + 2)$. Notice that if the choice $a * b = c$ generates 3 entries in the Cayley table then the number of entries the choice $a * b = c$ generates is the exact number adjacent to m in the equality $a * b = c$. Note the same result holds when $a * b = c$ generates 4 or 5 entries in the Cayley table. Now recall that all equalities generated by the choice $a * b = c$ are in the form of one of the equalities in X_j. Therefore, if the choice $a * b = c$ generates less than $3s$ entries in the Cayley table, then the choice $a * b = c$ must be equivalent to one of the following equalities in table 3.6 for $j = 0, 1, ...s - 1$.

Table 3.5. Iteration 3.5

$[a + (3j)m + j][*b + (3j)m + j] = [c + (3j)m + j]$
$[c + (3j + 1)m + j] * [a + (3j + 1)m + (j + 1)] = [b + (3j + 1)m + j]$
$[b + (3j + 2)m + j] * [c + (3j + 2)m + (j + 1)] = [a + (3j + 2)m + (j + 1)]$

Therefore, if the choice $a * b = c$ is equivalent to $[a + (3j)m + j][*b + (3j)m + j] = [c + (3j)m + j]$,then the choice $a * b = c$ generates $3j$ entries in the Cayley

24

table. Next, if the choice $a * b = c$ is equivalent to $[c + (3(j + 1))m + j] * [a + (3(j + 1))m + ((j + 1))] = [b + (3(j + 1))m + j]$ then the choice $a * b = c$ generates $3(j + 1)$ entries in the Cayley table. Next, if the choice $a * b = c$ is equivalent to $[b + (3(j + 2))m + j] * [c + (3j + 2)m + (j + 1)] = [a + (3j + 2)m + (j + 1)]$ then the choice $a * b = c$ generates $3j + 2$ entries in the Cayley table. It is important to note that if the choice $a * b = c$ generates $3j$, $3j + 1$ or $3j + 2$ entries in the Cayley table then these values must divide $3s$.

3.2   M-inverse loop of order 3k with a long inverse cycle

In this section we will devote our attention to m-inverse loops with a long inverse cycle of order $3k$. The goal of this section is to determine ways to fill out row zero when $n = 3(2k_1 + 1)$ for $k_1 \in Z^+$. Recall that each equality generated by the choice $a * b = c$ can be represented by one of the equalities in X_j for $j = 0, 1, ...s - 1$ where s is the smallest positive integer such that $s(3m + 1) \equiv 0$. Therefore, we refer to X_j to prove the following proposition that will assist us in filling out row zero in the Cayley table.

Proposition 8. *If $(Q, *)$ is a m-inverse loop of order n then there exists $t \in Z^+$ such that $t(3m + 1) \equiv 0$*

Proof. If $3m + 1 \equiv 0$ then we are done. Assume $3m + 1 \not\equiv 0$. We know that $i(3m + 1) \equiv a \; mod(n - 1)$ for $a \in Q$ and $a \neq e$. Recall that the order of Q is n. Let $i(3m + 1) \equiv a_i$ for $i = 1, 2, ..., n - 1$ and consider $n(3m + 1) \equiv a_n$. Now since there are only $n - 1$ choices this implies $n(3m + 1) \equiv i(3m + 1)$ where $n > i$. Therefore, $(n - i)(3m + 1) \equiv 0$ where $0 < n - i < n$. Therefore, there exist an integer $t \in Z^+$ such that $t(3m + 1) \equiv 0$

25

$\square$

Proposition 9. *Let $(Q, *)$ be a m-inverse loop of order n with a long inverse with the choice $a * b = c$ and $i \neq j$. Then $i(3m + 1) \not\equiv j(3m + 1)$.*

Proof. Note that $j - i > 0$ where $0 < i < j < s$ and s is the smallest positive integer such that $s(3m + 1) \equiv 0$. Assume that $i(3m + 1) \equiv j(3m + 1)$. This implies that $(j - i)3m + 1 \equiv 0$. However since $(j - i) < s$ and $(j - i) \not\equiv 0$, this is a contradiction since s is the smallest positive integer such that $s(3m + 1) \equiv 0$. $\square$

Lemma 3. *If $(Q, *)$ is a m-inverse loop of order n then the choice $a * b = c$ generates $3s$ or s entries in the Cayley table where s is the smallest positive integer such that $s(3m + 1) \equiv 0$. Note for m-inverse loops $s = (n - 1)/2$.*

Proof. With the choice $a * b = c$ we have already shown that at most $3s$ equalities hold. We show that if the choice $a * b = c$ generate less than $3s$ entries then the amount of entries generated by the choice $a * b = c$ is s. Let s be the smallest positive integer such that $s(3m + 1) \equiv 0$ and the choice $a * b = c$ generates t entries in the Cayley table such that $t < 3s$. It follows that t divides $3s$ and the choice $a * b = c$ is equivalent to one of the equalities in the the set below.

Table 3.6. Iteration 3.6

$[a + (3j)m + j][*b + (3j)m + j] = [c + (3j)m + j]$
$[c + (3(j + 1))m + j] * [a + (3(j + 1))m + (j + 1)] = [b + (3j) + 1)m + j]$
$[b + (3j + 2)m + j] * [c + (3j + 2)m + (j + 1)] = [a + (3j + 2)m + (j + 1)]$

Recall that $j = 0, 1, ...s - 1$. Therefore since s is the smallest positive integer such that $s(3m + 1) \equiv 0$, this implies that the choice $a * b = c$ is not equivalent to the first equality. Assume the choice $a * b = c$ is equivalent to the second equality. Therefore we obtain that $[3(j+1)](3m+1) \equiv 0$. This implies that the choice $a*b = c$ generates $3(j + 1)$ entries in the Cayley table and $3j + 1 \equiv xs$ for some $x \in Z^+$ since $s(3m + 1) \equiv 0$. If $x = 1$ then we are done. Assume $x > 1$; we know from previous work that $3(j + 1) < 3s$. Therefore $x = 2$. However since $3j + 1$ divides $3s$ $x \neq 2$, thus we conclude that $x = 1$. Therefore if the choice $a * b = c$ generates t entries in the Cayley table where $t < 3s$, then $t = s$. Next assume that the choice $a * b = c$ is equivalent to the third equality. Therefore we obtain that $[3j + 2](3m + 1) \equiv 0$. This implies that the choice $a*b = c$ generates $3j + 2$ entries in the Cayley table and $3j + 2 \equiv xs$ for some $x \in Z^+$ since $s(3m+1) \equiv 0$. If $x = 1$ then we are done. Assume $x > 1$; we know from previous work that $3j + 2 < 3s$. Therefore $x = 2$. However since $3j + 2$ divides $3s$ we must have $x \neq 2$. Thus we conclude that $x = 1$. Therefore if the choice $a * b = c$ generates t entries in the Cayley table where $t < 3s$, then $t = s$. $\square$

Proposition 10. *Let $(Q, *)$ be a m-inverse loop of order $n = 3k = 3(2k_1 + 1)$ and $(n - 1)/2$ be the smallest positive integer such that $((n - 1)/2)(3m + 1) \equiv 0$. Then $a * [a + k_1(3m + 1) + m + 1] = a + 2k_1(3m + 1) + 2m + 1$ generates $(n - 1)/2$ distinct entries in the Cayley table.*

Proof. Assume the choice $a * b = c$ generates $(n - 1)/2$ entries in the Cayley table. Recall from the previous proposition that $s \equiv 3j + 1$ or $s \equiv 3j + 2$ and $s = (n - 1)/2$. This implies that $s = 3k_1 + 1$. Therefore $s \equiv 3j + 1$ which implies that the choice $a * b = c$ is equivalent to the second equality in the set below.

Table 3.7. Iteration 3.7

$$[a + (3j)m + j] * [b + (3j)m + j] = [c + (3j)m + j]$$
$$[c + (3(j + 1))m + j] * [a + (3(j + 1))m + (j + 1)] = [b + (3j) + 1)m + j]$$
$$[b + (3j + 2)m + j] * [c + (3j + 2)m + (j + 1)] = [a + (3j + 2)m + (j + 1)]$$

Therefore $b \equiv a + j(3m+1) + m + 1$ and $c \equiv a + 2j(3m+1) = 2m + 1$. However since $3(j+1) \equiv 3k_1 + 1$ then $k_1 \equiv j$. Thus we conclude that $a * [a + k_0 + 1] = a + (2k_0 + 1)$ generates $(n - 1)/2$ distinct entries in the Cayley table where $k_0 = k_1(3m + 1) + m$.

$\square$

In the next proposition we study the product $0 * b = c$ for $b, c \in Q$ and consider the entries the product generates in row zero depending on whether they are even or odd.

Proposition 11. *Let $(Q, *)$ be a m-inverse loop of order n with a long inverse cycle where $s = (n - 1)/2$.*

1. If $0 * b = c$ generates $3s$ entries in the Cayley table with b even and c odd then the choice $0 * b = c$ generates 3 odd entries in row zero.

2. If $0 * b = c$ generates $3s$ entries in the Cayley table such that b and c are even then the choice $0 * b = c$ generates one odd and one even entry in row zero.

3. If $0 * b = c$ generates $3s$ entries in the Cayley table with b odd and c even then the choice $0 * b = c$ generates one even entry in row zero.

Proof. 1. Assume b is even and c is odd. We know that the first term in each equality from set X_j determines the row the entry will be inputted in. It has been proven that the first terms $0 + j(3m+1)$, $c + j(3m+1) + m$ and $b + j(3m+1) + 2m$ are unique, for $j =$

$0, 1..., ((n-1)/2)-1$ Therefore, we must determine which of these terms is congruent to zero since we are investigating entries in row zero. We are given one entry in row zero, $0*b = c$ which can also be written as $[0+0(3m+1)]*[b+0(3m+1)] = [c+0(3m+1)]$. Recall that each $j(3m+1)$ is unique for $j = 0, 1..., ((n-1)/2)-1$ and $0(3m+1) \equiv 0$. Now there are $(n-1)/2$ of the terms $j(3m+1)$ since $j = 0, 1..., ((n-1)/2)-1$. Note that $j(3m+1) \equiv a$ where $a \in Q$ is even . Since there are $n-1$ non-identity elements this implies that there exist $(n-1)/2$ even elements of Q. Therefore, since $0(3m+1) \equiv 0$ no other $j(3m+1)$ can be congruent to zero. Next we check to see if for some j, $c + j(3m+1) + m$ is congruent to zero. Recall that c and m are odd and $j(3m+1)$ is even; therefore $c + j(3m+1) + m \equiv a$ where a is even and $j = 0 : ((n-1)/2)$. This implies for some j, $c + j(3m+1) + m \equiv 0$. Finally we check to see if for some j, $b + j(3m+1) + 2m$ can be congruent to zero. Recall that b and $j(3m+1)$ are even and m is odd; therefore $b + j(3m+1) + m \equiv b$, where $b \in Q$ is even. Therefore, $b + j(3m+1) + 2m \equiv 0$ for some $j = 0 : (n-1)/2$. Notice that the entry associated with $c + j(3m+1) + m$ is $b + j(3m+1) + m$. Since b is even this entry is odd and the entry associated with $b + j(3m+1) + 2m$ is $j(3m+1) + 2m + 1$. Therefore, this entry is odd as well, so c, $b + j(3m+1) + m$ and $j(3m+1) + 2m + 1$ are the odd entries in row zero.

2. Assume b and c are even; again we know that each $j(3m+1)$, $c + j(3m+1) + m$ and $b+j(3m+1)+2m$ are unique for $j = 0, 1..., ((n-1)/2)-1$ and from the previous proof $j(3m+1) \not\equiv 0$ except when $j = 0$. Therefore, the terms $c + j(3m+1) + m$ and $b + j(3m+1) + 2m$ are the remaining choices for an entry in row zero. Consider $c + j(3m+1) + m$. Note that c and $j(3m+1)$ are even and m is odd; therefore $c + j(3m+1) + m$ is odd and cannot be congruent to zero. Finally we check $b + j(3m+1)+2m$ where b, $j(3m+1)$ and $2m$ are even. Therefore $c+j(3m+1)+m \equiv a$ and $a \in Q$ is even. Thus by the same logic as in the previous proof, for some j,

29

$b + j(3m + 1) + 2m \equiv 0$. Notice that the entry associated with $b + (3m + 1) + 2m$ is $j(3m + 1) + 2m + 1$. Therefore this entry is odd; thus c is even and for some j, $j(3m + 1) + 2m + 1$ is an odd entry in row zero.

3. Assume b is odd and c is even. Recall $j(3m + 1) \not\equiv 0$ except when $0 * b = c$. Now since c and $j(3m+1)$ are even and m is odd then $c + j(3m+1) + m$ is odd. Also since b and m are odd and $j(3m + 1)$ is even then $b + j(3m + 1) + 2m$ is odd. Therefore, $c + j(3m + 1) + m$ and $b + j(3m + 1) + 2m$ are both congruent to some odd element in Q. Thus neither term can be congruent to zero. Therefore, we conclude that c is the only entry generated in row zero where c is even.

□

Proposition 12. *Let $(Q, *)$ be a m-inverse loop of order n with a long inverse cycle with b even, c odd and the choice $0 * b = c$ generates $3(n - 1)/2$ entries in the Cayley table. Then the choice $0 * b = c$ generates no entries in row one.*

Proof. Assume b is even and c is odd. Observe that $j(3m + 1)$, $c + j(3m + 1) + m$, $b + j(3m + 1) + 2m$ for $j = 0, 1..., ((n - 1)/2) - 1$ are the terms that will determine what row the entries are inputted in. Therefore, one of the three terms must be congruent to one in order for the choice $0 * b = c$ to generate an entry in row 1. Note that $j(3m + 1) \equiv a_0$ and $a_0 \in Q$ is even; therefore $j(3m + 1) \not\equiv 1$. Secondly c and m are odd and $j(3m + 1)$ is even; therefore $c + j(3m + 1) + m \equiv a_1$ and $a_1 \in Q$ is even. Thus $c + j(3m + 1) + m \not\equiv 1$. Finally b, $j(3m + 1)$ and $2m$ are even; therefore $b + j(3m + 1) + 2m \equiv a_2$ and a_2 is even; thus $b + j(3m + 1) + 2m \not\equiv 1$. Therefore all the possible choices for rows are even. However 1 is odd. Thus the choice $0 * b = c$ generates no entries in row one.

□

Proposition 13. *Let $(Q, *)$ be a m-inverse loop of order n with a long inverse cycle such that b and c are even and $0 * b = c$ generates $3(n-1)/2$ entries in the Cayley table. Then the choice $0 * b = c$ generates one odd entry in row one.*

Proof. Assume b and c are even and $j(3m+1)$, $c+j(3m+1)+m$,$b+j(3m+1)+2m$ for $j = 0, 1..., ((n-1)/2) - 1$ are the terms that will determine what row the entries are inputted in. Therefore, one of the three terms must be equivalent to 1 in order for the choice $0 * b = c$ to generate an entry in row 1. Notice that $j(3m+1) \equiv a_0$ and $a_0 \in Q$ is even; therefore $j(3m+1) \not\equiv 1$. Secondly b, $j(3m+1)$ and $2m$ are even; therefore $b + j(3m+1) + 2m \equiv a_2$ and a_2 is even. Thus $b + j(3m+1) + 2m \not\equiv 1$. Finally c and $j(3m+1)$ are even and m is odd; therefore $c+j(3m+1)+m \equiv a_1$ and $a_1 \in Q$ is odd. Thus for some j, $c+j(3m+1)+m \equiv 1$ since $j = 0, 1..., ((n-1)/2) - 1$. Note that the entry associated with $c + j(3m+1) + m$ is $b + j(3m+1) + m$ which is an odd entry in row one.

$\square$

Proposition 14. *Let $(Q, *)$ be a m-inverse loop of order n with a long inverse cycle with b odd, c even and the choice $0 * b = c$ generates $3(n-1)/2$ entries in the Cayley table. Then the choice $0 * b = c$ generates one odd and one even entry in row one.*

Proof. Assume b is odd and c is even. Now we know that $j(3m+1)$, $c+j(3m+1)+m$ and $b + j(3m+1) + 2m$ are unique, where $j = 0, 1..., ((n-1)/2) - 1$. We have that $j(3m+1)$ is always congruent to some even element. Since b is odd and c even this implies that $c + j(3m+1) + m$ and $b + j(3m+1) + 2m$ are both congruent to some odd element in Q. Now since we are assuming that $(Q, *)$ is a m-inverse loop with long inverse cycle there exist only $(n-1)/2$ odd elements. This implies that there exist some j such that $c+j(3m+1)+m \equiv 1$ and $b+j(3m+1)+2 \equiv 1$. Notice that

31

the entry associated with $c + j(3m + 1) + m$ is $b + j(3m + 1) + m$. Since b is odd this entry is even; also the entry associated with $b + j(3m+1) + 2m$ is $j(3m+1) + 2m + 1$. Therefore, this entry is odd. Thus the choice $0 * b = c$ generates one odd and one even entry in row one. $\square$

Proposition 15. *Suppose $(Q, *)$ is a m-inverse loop of order n, $(n - 1)/2$ is the smallest positive integer such that $[(n - 1)/2](3m + 1) \equiv 0$ and row zero is filled out. Then all the even rows and columns are filled out and no odd entires are missing.*

Proof. Assume row zero is filled out and there exist the choice $a * b = c$ where a and b are even and c is odd. This implies that after row zero is filled out there remains an even row and an even column with a missing odd entry. Now recall that the first term of each equality in set X_j determines what row the entry is inputted in for $j = 0, 1..., ((n - 1)/2) - 1$. Recall that each $a + j(3m + 1)$, $b + j(3m + 1) + 2m$ and $c + j(3m+1) + m$ are unique and a and b are even. This implies that $a + j(3m+1) \equiv a_0$ and $b + j(3m+1) + 2m \equiv b_0$ for even $a_0, b_0 \in Q$. Also since c is odd, $c + j(3m+1) + m \equiv a_1$ for even $a_1 \in Q$. Therefore, since $j = 0, 1..., ((n - 1)/2) - 1$ then each term is congruent to zero for some j which is a contradiction since row zero is filled. $\square$

Now we present some number theoretic results that will be useful as we move forward. For completeness we include their proofs.

Proposition 16. *If $n = 3k$, $k \in Z^+$, then $3(n - 1)/2$ does not divide $n^2 - 3n + 2$.*

Proof. Note that $n^2 - 3n + 2$ is the amount of entries initially missing from the Cayley table when $(Q, *)$ is a m-inverse loop of order n.

Assume $3(n-1)/2$ divide $n^2 - 3n + 2$ where $3(n-1)/2$ and $n^2 - 3n + 2$ are both positive integers. This implies that $[(3(n-1)/2)]k_1 = n^2 - 3n + 2 = (n-1)(n-2)$ for some $k_1 \in Z^+$. Therefore, since $n = 3k$ then $3/2(k_1) = (n-2)$ and $3k_1 = 2(3k) - 2(2)$ thus $2(3k) - 3k_1 = 4$. This implies that $2k - k_1 = 4/3$. However since $2k - k_1 \in Z$ this is a contradiction since $4/3 \notin Z$. Therefore, $3(n-1)/2$ does not divide $n^2 - 3n + 2$.

$\square$

Proposition 17. If $n = 3k$, $k \in Z^+$ then $3(n-1)/2$ does not divide $[(n^2 - 3n + 2) - (n-1)/2]$

Proof. Assume $3(n-1)/2$ divide $n^2 - 3n + 2 - (n-1)/2$ where $3(n-1)/2$ and $n^2 - 3n + 2$ are both positive integers. This implies that $[(3(n-1)/2)]k_1 = n^2 - 3n + 2 = (n-1)(n-2) - (n-1)/2$ for some $k_1 \in Z^+$. Therefore, since $n = 3k$ then $3/2(k_1) = (n - 5/2)$ and $3k_1 = 2(3k) - 5$. Thus $2(3k) - 3k_1 = 5$. This implies that $2k - k_1 = 5/3$; however since $2k - k_1 \in Z$ this is a contradiction since $5/3 \notin Z$. Therefore, $3(n-1)/2$ does not divide $n^2 - 3n + 2$

$\square$

Proposition 18. If $n = 3k$, $k \in Z^+$ then $3(n-1)/2$ divides $(n^2 - 3n + 2) - (n-1)$

Proof. Let $n = 3(2k_1 + 1)$; this implies that $3(n-1)/2 = 3(3k_1 + 1)$ where $k_1 \in Z^+$. Consider $n^2 - 3n + 2 - (n-1) = (n-1)(n-2) - n - 1 = (n-1)(n-3)$. Since $n = 3(2k_1 + 1)$ then $n - 1 = 2(3k_1 + 1)$. Therefore $(n-1)(n-3) = [3(2k_1 + 1)][3(2k_1 + 1) - 2] = 3(3k_1 + 1)(4k_1)$. This implies that $3(n-1)/2$ divides $(n^2 - 3n + 2) - (n-1)$.

$\square$

Proposition 19. Let $(Q, *)$ be a m-inverse loop of order n with a long inverse cycle.

1. If $0 * b = c \in B$ and $0 * b_1 = c_1 \in B$ then $b - c \not\equiv b_1 - c_1$.

2. If $0 * b = c \in C$ and $0 * b_1 = c_1 \in C$ then $b - c \not\equiv b_1 - c_1$.

Proof. 1. Assume $0*b = c$, $0*b_1 = c_1$ and $b - c \equiv b_1 - c_1$ where b, b_1, c, c_1 are even. Since $0 * b = c \in B$ and $0 * b_1 = c_1 \in B$ then each equality generates an entry in row zero other than c and c_1 respectively. This implies that for some $j, i = 0, 1, ..., (n - 1/2) - 1$ we have $c + j(3m + 1) + m \equiv 0$ and $c_1 + i(3m + 1) + m \equiv 0$ where $b + j(3m + 1) + m$ and $b_1 + i(3m + 1) + m$ are the entries in row zero respectively. This implies that $-c \equiv j(3m + 1) + m$ and $-c_1 \equiv i(3m + 1) + m$. Therefore the entries can be rewritten as $b - c$ and $b_1 - c_1$. Recall that we assume that $b - c \equiv b_1 - c_1$, hence $0 * b = c$ and $0 * b_1 = c_1$ generate the same entry in row zero which is a contradiction. Thus $b - c \not\equiv b_1 - c_1$.

2. Assume $0 * b = c$, $0 * b_1 = c_1$ and $b - c \equiv b_1 - c_1$ where b, b_1 are odd and $, c, c_1$ are even. Since $0 * b = c \in C$ and $0 * b_1 = c_1 \in C$ then each equality respectively generates two entries in row 1. This implies that for some $j, i = 0, 1, ..., (n - 1/2) - 1$ we have $c + j(3m + 1) + m \equiv 1$ and $c_1 + i(3m + 1) \equiv 1$ where $b + j(3m + 1) + m$ and $b_1 + i(3m + 1) + m$ are the entries in row one respectively. This implies that $1 - c \equiv j(3m + 1) + m$ and $1 - c_1 \equiv i(3m + 1) + m$. Therefore the entries can be rewritten as $(b - c) + 1$ and $(b\_c_1) + 1$. Recall that we assume that $b - c \equiv b_1 - c_1$. This implies that $0 * b = c$ and $0 * b_1 = c_1$ generates the same entry in row one which is a contradiction. Thus $b - c \not\equiv b_1 - c_1$.

$\square$

Now we use the previous propositions to ascertain all the ways that we can fill out row zero for a m-inverse loop of order $3k$ with a long inverse cycle. Once a particular manner for completing row zero is determined, the next objective is to determine what entries in row one are missing. Once this information is obtain we then decide if the completion of row one leads to the construction of a Cayley table. In order to determine how many ways we can fill row zero we must consider the

non-identity elements in Q. Then we determine the number of missing entries in row zero, where the missing entries are characterized as odd or even. Since the order of Q is n there are $n - 1$ non-identity elements. Recall that $n = 3k = 3(2k_1 + 1)$ and $n - 1 = 3(2k_1) + 2 = 2(3k_1 + 1)$. Therefore, there are $3k_1 + 1$ odd and $3k_1 + 1$ even entries in each row. Since we assumed that $(Q, *)$ is a m-inverse loop with long inverse cycle, we are given two entries in each row $a * e = a$ and $a * (a + 1) = e$ where $a \in Q$. This implies that we are given $3n - 2$ entries in the Cayley table. This implies there are $n^2 - 3n + 2$ missing entries. Note that if the choice $a * b = c$ generates $(n - 1)/2$ entries in the Cayley table then $0 * (k_0 + 1) = 2k_0 + 1$ or $1 * [1 + (k_0 + 1)] = 1 + (2k_0 + 1)$.

Recall that thus far we are given the choices $0 * e = 0$ and $0 * 1 = e$. Therefore we are only given one even non-identity element. This implies that $3k_1$ even entries and $3k_1 + 1$ odd entries are missing in row zero. If we attempt to construct the Cayley table such that for all $a, b, c \in Q$, $a * b = c$ generates $3(n - 1)/2$ entries in the Cayley table then $3(n - 1)/2$ must divide $n^2 - 3n + 2$. However it has been proven in a previous proposition that $3(n - 1)/2$ does not divide $n^2 - 3n + 2$. However, $3(n - 1)/2$ divides $(n^2 - 3n + 2) - (n - 1)$. Therefore we need $0 * (k_0 + 1) = (2k_0 + 1)$ or $1 * [1 + (k_0 + 1)] = 1 + (2k_0 + 1)$ which generates $(n - 1)/2$ entries each in the Cayley table respectively. Therefore, if a m-inverse loop of order $3k$ exists then $0 * (k_0 + 1) = (2k_0 + 1)$ and $1 * [1 + (k_0 + 1)] = 1 + (2k_0 + 1)$ which implies that for row zero we are given $0 * 1 = e$, $0 * e = 0$ and $0 * (k_0 + 1) = (2k_0 + 1)$ where $2k_0 + 1$ is some odd entry in row zero. Thus for a m-inverse loop of order $3(2k_1 + 1)$ there are only $3k_1$ odd missing and $3k_1$ even missing entries in row zero.

Now recall that the choice $0 * b = c$ generates either 3 odd,1 odd 1 even, or 1 even entry in row zero. Therefore, let's define A as the set of all choices $0 * b = c$ that generate exactly 3 odd entries in row zero. Define B as the set of all choices $0 * b = c$

that generate 1 odd and 1 entry in row zero. Finally, define C as the set of all choices $0 * b = c$ that generate 1 even entry in row zero. Next we determine the maximum amount of equalities that can be used from A in order to complete row zero. Each $0 * b = c$ from A will only generate 3 odd entries in row zero and we know that there are $3k_1$ odd missing entries. Therefore, the maximum number of equalities that can be utilized from A to complete row zero is k_1. The following table shows the number of equalities derived when $0 * b = c$ is taken from set A, B and B. We designate forms $1 - k_1$ to all possible combinations.

Table 3.8. Completion of row zero for the order of $3k$

Form	$0 * b = c$ from A	$0 * b = c$ from B	$0 * b = c$ from C
1	k_1	0	$3k_1$
2	$k_1 - 1$	3	$3k_1 - 3$
3	$k_1 - 2$	6	$3k_1 - 6$
4	$k_1 - 3$	9	$3k_{-}1$
...	....	.....	
$k_1 - 1$	$k_1 - (k_1 - 2)$	$3(k_1 - 2)$	$3k_1 - 3(k_1 - 2)$
k_1	$k_1 - (k_1 - 1)$	$3(k_1 - 1)$	$3k_1 - [3(k_1 - 1)]$

Next we consider if it is possible to fill row zero with equalities only from set B. Note that the equalities from set B generates 1 odd and 1 even entry in row zero. Since there are $3k_1$ odd and $3k_1$ even missing entries in row zero then we can have $3k_1$ equalities from B; therefore there are $k_1 + 1$ possible ways of selecting equalities from set A, B, and C to complete row zero.

3.2.1 M-inverse loops of order 15 with a long inverse cycle

We now apply the information that has been acquired to determine if a m-inverse loop with a long inverse cycle exist when $n = 15$ where $Q = e, 0, 1....13$. First we assume that such a structure exists where $(n-1)/2$ is the smallest positive integer such that $[(n-1)/2](3m+1) \equiv 0$. With the assistance of Mathlab we determined that the choice $a * b = c$ generates the same equalities regardless of what m is chosen when $3m + 1 \not\equiv 0$. Recall that since $n = 3k$, then $0 * (k_0 + 1) = (2k_0 + 1)$ and $1 * [1 + (k_0 + 1)] = 1 + (2k_0 + 1)$. Hence we have the following entries in the Cayley table: $0 * e = e, 0 * 1 = e$ and $0 * 10 = 5$. Recall that $n = 15 = 3(5)$ where $5 = 2k_1 + 1$; this implies that $k_1 = 2$. Therefore, there are $3(2)$ odd and $3(2)$ even missing entries in row zero. We also know that there are $2 + 1$ ways to complete zero. As previously stated, the first form that can be employed to fill row zero will consist of k_1 equalities from set A and in this case $k_1 = 2$. The following table displays three different ways to complete row zero and for each form we have the choice $0 * 10 = 5$.

Table 3.9. Completion of row zero for the order of 15

Form	Number of $0 * b = c \in A$	Number of $0 * b = c \in B$	Number of $0 * b = c \in C$
1	2	0	6
2	1	3	3
3	0	6	0

Consider form 1 and recall that if $0 * b_i = c_i \in C$ then b_i odd, c_i even and $b_i - c_i \not\equiv b_j - c_j$. Therefore, let $0 * b_i = c_i$ for $i = 1, 2..., 6$. The table below displays the possible values for c_i when b_i is odd for $i = 1, 2..., 6$.

Table 3.10. Equalities 3.10

$0 * 3 = c_1 =$	2	4	6	8	10	12
$0 * 5 = c_2 =$	2	4	6	8	10	12
$0 * 7 = c_3 =$	2	4	6	8	10	12
$0 * 9 = c_4 =$	2	4	6	8	10	12
$0 * 11 = c_5$	2	4	6	8	10	12
$0 * 13 = c_6$	2	4	6	8	10	12

Let $0 * 3 = 2$; this implies that $5 - c_2$, $7 - c_3$, $9 - c_4$, $11 - c_5$ and $13 - c_6$ cannot be congruent to 1. And c_i cannot equal 2 for $i = 2, ..., 6$. Therefore, we obtain the following table.

Table 3.11. Equalities 3.11

$0 * 5 = c_2 =$			6	8	10	12
$0 * 7 = c_3 =$		4		8	10	12
$0 * 9 = c_4 =$		4	6		10	12
$0 * 11 = c_5$		4	6	8		12
$0 * 13 = c_6$		4	6	8	10	

Observe that if $0 * 3 = 2$, then $0 * 5 = 6, 8, 10$, or 12. Let $0 * 5 = 6$; this implies that $7 - c_3$, $9 - c_4$, $11 - c_5$ and $13 - c_5$ cannot be congruent to -1. Moreover $c_4.....c_6$ cannot equal 6. Therefore, we obtain the following table.

Table 3.12. Equalities 3.12

$0*7 = c_3 =$		4			10	12
$0*9 = c_4 =$		4				12
$0*11 = c_5$		4		8		
$0*13 = c_6$		4		8	10	

Let $0*9 = 4$; this implies that $0*11 = 8$ and $0*13 = 10$. Notice that $11 - 8 = 13 - 10$. Therefore $0*9 \neq 4$. Let $0*9 = 12$; this implies that $0*7 \neq 10$. Therefore $0*7 = 4$ and $0*11 = 8$. However $7 - 4 = 11 - 8$. Thus $0*9 \neq 12$ which implies that $0*5 \neq 6$.

Next let $0*3 = 2$ and $0*5 = 8$, with these choices we obtain the following table.

Table 3.13. Equalities 3.13

$0*7 = c_3 =$		4				12
$0*9 = c_4 =$		4	6		10	
$0*11 = c_5$		4	6			12
$0*13 = c_5$		4	6		10	

Let $0*7 = 4$, $0*3 = 2$ and $0*5 = 8$; this implies that $0*9 = 10$, $0*13 = 6$ and $0*11 = 12$. Therefore, $0*7 \neq 4$. Let $0*7 = 12$, $0*3 = 2$ and $0*5 = 8$; this implies that $0*11 = 4$ or $0*11 = 6$. Assume $0*11 = 4$; this implies that $0*13 = 10$ and $0*9 = 6$. Therefore, $0*11 \neq 4$. Next assume $0*11 = 6$; this implies that $0*13 = 10$ and $0*9 = 4$. Therefore $0*7 \neq 12$. Thus we conclude that $0*5 \neq 8$. Let $0*3 = 2$ and $0*5 = 10$. Therefore, we obtain the following table as listed below.

Table 3.14. Equalities 3.14

$0*7 = c_3 =$	4		8		
$0*9 = c_4 =$	4	6			12
$0*11 = c_5$	4	6	8		12
$0*13 = c_5$		6	8		

Let $0*7 = 4$; this implies that $0*9 = 12$, $0*11 = 6$ and $0*13 = 8$. Therefore $0*7 \neq 4$. Let $0*7 = 8$; this implies that $0*13 = 6$. Consider $0*11 = c_5$; $c_5 = 4$ or $c_5 = 12$. If $c_5 = 4$ then $11 - 4 = 13 - 6$. Therefore $0*11 \neq 4$. Assume $c_5 = 12$; this implies $0*11 = 12$. Therefore $0*7 \neq 8$. Furthermore we conclude that $0*5 \neq 10$.

Letting $0*3 = 2$ and $0*5 = 12$ we obtain the following table.

Table 3.15. Equalities 3.15

$0*7 = c_3 =$	4		8	10	
$0*9 = c_4 =$	4	6	10		
$0*11 = c_5$		6	8		
$0*13 = c_5$	4		8	10	

Let $0*11 = 6$; this implies that $0*9 = 10$,$0*7 = 4$ and $0*13 = 8$. Thus if $0*3 = 2$ there is no choice for $0*5 = c_2$. We conclude that $0*3 \neq 2$. Note to show that $0*3 \neq 4, 6, 8, 10,$ or 12 we follow the same steps. Therefore, form 1 does not lead to the construction of a Cayley table.

Now let's draw our attention to form 3 where we have $0*10 = 5$ and six equalities from B. From the previous propositions we discover that equalities from B and C satisfy the same property: $b - c \not\equiv b_1 - c_1$. Therefore, if we cannot have 6

equalities from C then 6 equalities from B is also not possible thus the final form does not hold. We have eliminated 2 of the 3 forms to fill row zero, now we investigate form 2. Observe that form 2 has the choice $0*10 = 5$, one equality from A, three equalities from B and three equalities from C. Therefore, in order to fill row zero we need a total of 8 equalities where each $0 * b = c$ generates 21 entries in the Cayley table, except $0 * 10 = 5$ which generates 7 entries in the Cayley table. This implies that the total amount of entries generated in the Cayley table after row zero is completed is 154. Recall that in order for a m-inverse loop of order 15 to exists $1 * 11 = 6$ where this equality generates 7 entries in the Cayley table. This implies we now have $154 + 6$ of 182 missing entries. Notice that we need 21 entries to complete the Cayley table. Therefore, since we are focusing on completing row zero and row one we need to determine how many of the 154 entries have been placed into row 1. We know that only the choices $0 * b = c \in B$ and $0 * b = c \in C$ generate entries in row 1, where $0 * b = c \in B$ generates 1 odd entry in row 1 and $0 * b = c \in C$ generate 1 odd entry and 1 even entry in row 1. Therefore, we have a total of 10 entries inputted in row 1 after row zero is filled, where 6 entries are odd and 4 are even. This implies that in order to complete the Cayley table there must exist the choice $1 * b = c$ that generates 3 even entries in row one. With the help of Mathlab we determined that if the choice $1 * b = c$ generates three even entries in row one after row zero is filled then the choice $1 * b = c$ generates either the entries $2, 4, 12$ or $0, 8, 10$ in row one. Also with the help of Mathlab we determined if $0 * b = c \in A$ then the choice $0 * b = c$ generates one of the following set of odd entries in row zero:$(5, 11, 13)$, $(1, 5, 9)$, $(3, 5, 7)$, $(1, 3, 11)$ or $(7, 9, 13)$. However since $0 * 10 = 5$, the only options for entries in row zero obtained by the choice $0 * b = c \in A$ are: $(1, 3, 11)$ and $(7, 9, 13)$. Therefore, we conclude that there are four cases which have to be investigated in order to determine if the Cayley

41

table can be constructed. Note that we will only discuss case 1 and the investigation of all other cases lead to the same conclusion. Here are the cases:

1. The choice $0 * b = c \in A$ generates the entries $1, 3, 11$ in row zero and the choice $1 * h = k$ generates the entries $2, 4, 12$ in row one.

2. The choice $0 * b = c \in A$ generates the entries $1, 3, 11$ in row zero and the choice $1 * h = k$ generates the entries $0, 8, 10$ in row one.

3. The choice $0 * b = c \in A$ generates the entries $7, 9, 13$ in row zero and the choice $1 * h = k$ generates the entries $2, 4, 12$ in row one.

4. The choice $0 * b = c \in A$ generates the entries $7, 9, 13$ in row zero and the choice $1 * h = k$ generates the entries $0, 8, 10$ in row one.

Case 1

Assume $0 * b = c \in A$ generates the entries $1, 3, 11$ in row zero; therefore we need $0 * b_i = c_i \in B$ for $i = 1, .., j = 0, 1..., ((n-1)/2) - 13$ such that the choice $0 * b_1 = c_1$ generates the entry 7 in row zero, the choice $0 * b_2 = c_2$ generates the entry 9 in row zero, and the choice $0 * b_3 = c_3$ generates the entry 13 in row zero. The next step is to determine the value of b_i and to do so we need the following iterations. Recall that each equality that is generated by the choice $0 * b = c$ can be represented by one of the equalities in the set below for $j = 0, 1..., ((n-1)/2) - 1$.

Table 3.16. Iteration 3.16

$[0 + j(3m + 1)] * [b + j(3m + 1)] = [c + j(3m + 1)]$
$[c + j(3m + 1) + m] * [0 + j(3m + 1) + (m + 1)] = [b + j(3m + 1) + m]$
$[b + j(3m + 1) + 2] * [c + j(3m + 1) + (2m + 1)] = [0 + j(3m + 1) + (2m + 1)]$

42

First we determine the choices for an entry in row zero. We are given $[0 + 0(3m+1)] * [b+0(3m+1)] = [c+0(3m+1)]$. Therefore since $(n-1)/2$ is the smallest positive integer such that $[(n-1)/2](3m+1) \equiv 0$. We conclude that $j(3m+1) \not\equiv 0$ for $j = 1, 2..., ((n-1)/2) - 1$. Notice that for $0 * b_i = c_i \in B$, b_i and c_i are even; thus the only choice for an entry in row zero is $[b+j(3m+1)+2m] * [c+j(3m+1)+2m+1] = [j(3m+1)+2m+1]$ when $0 * b_i = c_i \in B$ for $i = 1, 2, 3$.

Now we determine to which element of Q is b_i congruent to when the choice $0 * b_i = c_i$ generates the entry 7 in row zero. If $0 * b_i = c_i$ generates the entry 7 in row zero then for some j, $b_i + j(3m+1) + 2m \equiv 0$ and $j(3m+1) + 2m + 1 \equiv 7$; this implies $j(3m+1) + 2m \equiv 6$. Therefore $b_i + 6 \equiv 0$; thus $b_i \equiv 8$ since the arithmetic is modulo 14. This implies that $0 * 8 = c_i$ generates the entry 7 in row zero where $0 * (c_i + 7) = 7$.

Next we determine to which element of Q is b_i congruent to when the choice $0 * b_i = c_i$ generates the entry 9 in row zero. If $0 * b_i = c_i$ generates the entry 9 in row zero then for some j, $b_i + j(3m+1) + 2m \equiv 0$ and $j(3m+1) + 2m + 1 \equiv 9$. This implies $j(3m+1) + 2m \equiv 8$. Therefore, $b_i + 8 \equiv 0$ and $b_i \equiv 6$ since the arithmetic is modulo 14. This implies that $0 * 6 = c_i$ generates the entry 9 in row zero where $0 * (c_i + 9) = 9$.

Finally we determine to which element of Q is b_i congruent to when the choice $0 * b_i = c_i$ generates the entry 13 in row zero. If $0 * b_i = c_i$ generates the entry 13 in row zero then for some j, $b_i + j(3m+1) + 2m \equiv 0$ and $j(3m+1) + 2m + 1 \equiv 13$. This implies $j(3m+1) + 2m \equiv 12$; therefore $b_i + 12 \equiv 0$ and $b_i \equiv 2$ since the arithmetic is modulo 14. This implies that $0 * 2 = c_i$ generates the entry 13 in row where $0 * c_i + 13 = 13$. Now that we have determined the value to which b_i is congruent to let's consider row one. Recall that we need 3 even entries in row 1. Therefore, we have to choose $0 * b = c \in C$ in such a way that the equality does not generate $1 * 11$

since we know that $1 * 11 = 6$. Also we do not want the equality to generate the same even entries that will be generated by the choice $1 * b = c$. Therefore since we have the choice $1 * b = c$ that generates $2, 4, 12$ this implies that $0 * b_i = c_i \in C$ $i = 1, 2, 3$ must generate $0, 8, 10$ in row one respectively. Next we determine what conditions are necessary for $0 * b = c$ to generate 0, 8, or 10 in row one if $0 * b = c \in C$. Consider the following iteration. Recall that each equality that is generated by $0 * b = c$ can be represented by one of the equalities in the set below for $j = 0, 1..., ((n-1)/2) - 1$.

Table 3.17. Iteration 3.17

$[0 + j(3m + 1)] * [b + j(3m + 1)] = [c + j(3m + 1)]$
$[c + j(3m + 1) + m] * [0 + j(3m + 1) + (m + 1)] = [b + j(3m + 1) + m]$
$[b + j(3m + 1) + 2] * [c + j(3m + 1) + (2m + 1)] = [0 + j(3m + 1) + (2m + 1)]$

Assume $0 * b = c \in C$; this implies that our choices for an entry in row 1 are determined by the terms $c + j(3m + 1) + m$ and $b + j(3 + m + 1) + 2m$ since $j(3m + 1) \not\equiv 1$ because $j(3m + 1)$ is even for $j = 0, 1..., ((n-1)/2) - 1$. Recall that b,m are odd and c is even. Therefore the only possible even entry in row 1 is $[c + j(3m + 1) + m] * [j(3m + 1) + m + 1] = [b + j(3m + 1) + m]$ for $j = 0, 1..., ((n-1)/2) - 1$.

First we determine the choices $0 * b = c \in C$ that generate the entry 0 in row 1. If the choice $0 * b = c$ generates the entry 0 in row 1 then for some j, $c + j(3m + 1) + m \equiv 1$ and $b + j(3m + 1) + m \equiv 0$; this implies $1 - c \equiv j(3m + 1) + m$ and $-b \equiv j(3m + 1) + m$. Therefore $c \equiv b + 1$ and $0 * b = b + 1$ generates the entry 0 in row 1. Next we determine the choice $0 * b = c \in C$ that generates the entry 8 in row 1. If the choice $0 * b = c$ generates the entry 8 in row 1 then for some j, $c + j(3m + 1) + m \equiv 1$ and $b + j(3m + 1) + m \equiv 8$; this implies $1 - c \equiv j(3m + 1)$

44

and $8 - b \equiv j(3m + 1) + m$. Therefore $c \equiv b + 7$ and $0 * b = b + 7$ generate the entry 8 in row 1. Finally we determine the choice $0 * b = c \in C$ that generate the entry 10 in row 1. If the choice $0 * b = c$ generates the entry 10 in row 1 then for some j, $c + j(3m + 1) + m \equiv 1$ and $b + j(3m + 1) + m \equiv 10$; this implies $1 - c \equiv j(3m + 1)$ and $10 - b \equiv j(3m + 1) + m$. Therefore $c \equiv b + 5$ and $0 * b = b + 5$ generates the entry 10 in row 1.

Recapping, we have chosen one equality $0 * b = c$ from A where $0 * b = c$ generates the entries $1, 3, 11$ in row zero, three equalities $0 * b = c$ from B as follows, $0 * 8 = c$ which generates the entry 7 in row zero since $0 * (c + 7) = 7, 0 * 6 = c_1$ which generates the entry 9 in row zero since $0 * (c_1 + 9) = 9, 0 * 2 = c_2$ which generates the entry 13 in row zero since $0 * (c_2 + 13) = 13$. Hence all the odd entries have been obtained and three even entries in row zero. Therefore, to obtain the remaining even entries in row zero we need three equalities $0 * b = c$ from C that respectively must generate 0,8 and 10 in row one. Therefore if $(Q, *)$ is a m-inverse loop of order 15 such that $3m + 1 \not\equiv 0$, the choice $0 * b = c$ generates the entries $(1, 3, 11)$ in row zero and $1 * h = k$ generates the entries $(2, 4, 12)$ in row one. Then the following set of equalities must hold.

Table 3.18. Iteration 3.18

$0 * 8 = c$
$0 * (c + 7) = 7$
$0 * 6 = c_1$
$0 * (c_1 + 9) = 9$
$0 * 2 = c_2$
$0 * (c_2 + 13) = 13$
$0 * c_3 = c_3 + 1$
$0 * c_4 = c_4 + 5$
$0 * c_5 = c_5 + 7$

45

Note that the proof for any applicable value of c where $0 * 8 = c$ is similar to the proof that will be given below so we will only show the case when $c = 2$. The goal of this proof is to investigate if the previous equalities hold can we construct a Cayley table associated with Q. Recall that $0 * 8 = c$, $0 * 6 = c_1$ and $0 * 2 = c_2$ are from set B and $0 * c_3 = c_3 + 1$, $0 * c_4 = c_4 + 5$, $0 * c_5 = c_5 + 7$ are from set C. Therefore, c, c_1, c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are even and c_i is odd where $c_i \not\equiv 1$ for $i = 3 : 5$. The table below displays the possible choices for an entry in the Cayley table . For example since $0 * 8 = c$ the table shows that $0 * 8 = c = 2, 4, 6, 10$ or 12 where 0 and 8 are excluded since $(Q, *)$ is a loop. Also since $c_i \not\equiv 1$ this implies that $c_3 + 1 \neq 2$, $c_4 + 1 \neq 6$ and $c_5 + 7 \neq 8$.

Table 3.19. Equalities 3.19

$c =$	2	4	6	10	12
$c_1 =$	2	4	8	10	12
$c_2 =$	4	6	8	10	12
$c_3 + 1 =$	4	6	8	10	12
$c_4 + 5 =$	2	4	8	10	12
$c_5 + 7 =$	2	4	6	10	12

Case 1a

Let $c = 2$; this implies that $0 * 8 = 2$ and $0 * 9 = 7$. Recall that $c, c_1, c_2, c_3 + 1, c_4 + 5$ and $c_5 + 7$ are even; c_i is odd and $c_i \not\equiv 9$ for $i = 3, 4, 5$. Also that $6 - c_1 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 8 - 2$ since $0 * 8 = c$, $0 * 6 = c_1$ and $0 * 2 = c_2$ are from B. Thus the remaining choices for c_1, c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are as listed below.

Table 3.20. Equalities 3.20

$c_1 =$		4	8	10	12
$c_2 =$	4	6	8		12
$c_3 + 1 =$	4	6	8		12
$c_4 + 5 =$		4	8	10	12
$c_5 + 7 =$		4	6	10	12

Notice from the above table if $0 * 8 = 2$ then $0 * 6 = 4$, $0 * 6 = 8$, $0 * 6 = 10$ or $0 * 6 = 12$. Let $0 * 6 = 4$; this implies that $0 * 13 = 9$ and therefore c_2, $c_3 + 1$, $c_4 + 5$ cannot equal 4. Moreover c_i cannot be congruent to 13 for $i = 3, 4, 5$ and $2 - c_2 \not\equiv 2$. Thus the remaining choices for c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are as listed below.

Table 3.21. Equalities 3.21

$c_2 =$		6	8		12
$c_3 + 1 =$		6	8		12
$c_4 + 5 =$			8	10	12
$c_5 + 7 =$				10	12

Observe that if $0 * 8 = 2$ and $0 * 6 = 4$ then $c_5 + 7 = 10$ or $c_5 + 7 = 12$. Let $c_5 + 7 = 10$; this implies that $0 * 3 = 10$ and by the same logic the remaining choices for c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are as listed below.

Table 3.22. Equalities 3.22

$c_2 =$		6	8		12
$c_3 + 1 =$		6	8		12
$c_4 + 5 =$					12

Therefore, from the previous table, $c_4 + 5 = 12$; this implies $0*7 = 12$ so again by the same logic the remaining choices for $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are as listed below.

Table 3.23. Equalities 3.23

$c_2 =$			6			
$c_3 + 1 =$			6			

The previous table implies that $c_2 \equiv c_3 + 1$ which is a contradiction since the choice for c_2 and $c_3 + 1$ are unique. Therefore, if $0*8 = 2$ and $0*6 = 4$ then $c_5 + 7 \neq 10$. Next let $0*8 = 2$, $0*6 = 4$ and $c_5 + 7 = 12$. Therefore, the remaining choices for c_2, $c_3 + 1$ and $c_4 + 5$, are as listed below.

Table 3.24. Equalities 3.24

$c_2 =$			6	8		
$c_3 + 1 =$				8		
$c_4 + 5 =$				8		

Notice that $c_4 + 5 \equiv c_3 + 1$ which is a contradiction since the choice for $c_4 + 5$ and $c_3 + 1$ are unique. Therefore if $0*8 = 2$ and $0*6 = 4$ then $c_5 + 7 \neq 10$ or 12. This implies that if $0*8 = 2$ then $0*6 \neq 4$.

Case 1b

Let $0*8 = 2$ and $0*6 = 8$; this implies that $0*9 = 7$ and $0*3 = 9$. Recall that c,c_1, c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are even and c_i is odd for $i = 3, 4, 5$. Therefore,

48

c_1, c_2, $c_3 + 1$, $c_4 + 5$ cannot equal 2 or $c_4 + 5 \neq 8$, $c_i \not\equiv 9$ or $c_i \not\equiv 3$ for $i = 3, 4, 5$ and

$6 - c_1 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 6 - 8$ since $0 * 8 = c$, $0 * 6 = c_1$ and

$0 * 2 = c_2$ are from B. Therefore, the remaining choices for c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$

are as listed below.

Table 3.25. Equalities 3.25

$c_2 =$		6			12
$c_3 + 1 =$		6			12
$c_4 + 5 =$		4		10	12
$c_5 + 7 =$		4	6		12

From the new table we conclude if $0 * 8 = 2$ and $0 * 6 = 8$ then $0 * c_3 = c_3 + 1 = 6$

or $0 * c_3 = c_3 + 1 = 12$. Let $0 * c_3 = 6$; this implies that $0 * 5 = 6$ and by the same

logic used to determine the previous table we obtain the following table.

Table 3.26. Equalities 3.26

$c_2 =$					12
$c_4 + 5 =$		4			12
$c_5 + 7 =$		4			

Therefore from the new table $c_2 = 12$; thus $0 * 2 = 12$ and we obtain the table

below.

Table 3.27. Equalities 3.27

$c_4 + 5 =$		4		
$c_5 + 7 =$		4		

Therefore $c_4 + 5 = c_5 + 7$ which is a contradiction since the choices $c_4 + 5$ and $c_5 + 7$ are unique. Therefore, if $0 * 8 = 2$ and $0 * 6 = 8$ then $0 * c_3 \neq 6$. Let $0 * c_3 = 12$; this implies that $0 * 11 = 12$. Therefore we obtain the following table.

Table 3.28. Equalities 3.28

$c_2 =$		6		
$c_4 + 5 =$		4	10	
$c_5 + 7 =$			6	

Therefore $c_2 = c_5 + 7$, which is a contradiction. Thus if $0 * 8 = 2$ and $0 * 6 = 8$ then $0 * c_3 \neq 6$ or $0 * c_3 \neq 12$. This implies that if $0 * 8 = 2$ then $0 * 6 \neq 8$.

Case 1c

Assume $0 * 8 = 2$ and $0 * 6 = 10$; this implies that $0 * 9 = 7$ and $0 * 5 = 9$. Recall that c, c_1, c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are even and c_i is odd for $i = 3, 4, 5$. Therefore, c_1, c_2, $c_3 + 1$, $c_4 + 5 \neq 2$ or $c_4 + 5 \neq 10$, $c_i \not\equiv 9$ or $c_i \not\equiv 5$ for $i = 3, 4, 5$ and $6 - c_1 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 6 - 10$ since $0 * 8 = c$, $0 * 6 = c_1$ and $0 * 2 = c_2$ are from B. The remaining choices for c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are as listed below.

50

Table 3.29. Equalities 3.29

$c_2 =$	4		8		12
$c_3 + 1 =$	4		8		12
$c_4 + 5 =$		4	8		12
$c_5 + 7 =$		4	6		

The above table indicates that if $0 * 8 = 2$ and $0 * 6 = 10$ then $c_5 + 7 = 4$ or 6. Let $c_5 + 7 = 4$ then we obtain the following table.

Table 3.30. Equalities 3.30

$c_2 =$			8		
$c_3 + 1 =$			8		
$c_4 + 5 =$			8		12

This implies that $c_2 = c_3 + 1$ which is a contradiction. Therefore if $0 * 8 = 2$ and $0 * 6 = 10$ then $c_5 + 7 \neq 4$. Now let $c_5 + 7 = 6$ then we obtain the following table.

Table 3.31. Equalities 3.31

$c_2 =$	4		8		12
$c_3 + 1 =$	4		8		12
$c_4 + 5 =$			8		12

This implies that if $0 * 8 = 2$, $0 * 6 = 10$ and $c_5 + 7 = 6$ then $c_4 + 5 = 8$ or $c_4 + 5 = 12$. Let $c_4 + 5 = 8$ then we obtain the following table.

Table 3.32. Equalities 3.32

$c_2 =$					12
$c_3 + 1 =$					12

Therefore, $c_2 = c_3 + 1$ which is a contradiction. This implies that if $0 * 8 = 2$, $0 * 6 = 10$ and $c_5 + 7 = 6$ then $c_4 + 5 \neq 8$. If $c_4 + 5 = 12$ then we obtain the following table.

Table 3.33. Equalities 3.33

$c_2 =$	4				
$c_3 + 1 =$	4				

This implies that $c_2 = c_3 + 1$ which is a contradiction. This implies that if $0 * 8 = 2$, $0 * 6 = 10$ and $c_5 + 7 = 6$ then $c_4 + 5 \neq 8$ or $c_4 + 5 \neq 12$. Therefore, if $0 * 8 = 2$ then $0 * 6 \neq 10$.

Case 1d

Assume $0 * 8 = 2$ and $0 * 6 = 12$; this implies that $0 * 9 = 7$ and $0 * 7 = 9$. Recall that c, c_1, c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are even and c_i is odd for $i = 3, 4, 5$. Therefore, c_1, c_2, $c_3 + 1$, $c_4 + 5 \neq 2$ or $c_4 + 5 \neq 12$, $c_i \not\equiv 9$ or $c_i \not\equiv 7$ for $i = 3, 4, 5$ and $6 - c_1 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 8 - 2$ and $2 - c_2 \not\equiv 6 - 12$ since $0 * 8 = c$, $0 * 6 = c_1$ and $0 * 2 = c_2$ are from B. Thus the remaining choices for c_2, $c_3 + 1$, $c_4 + 5$ and $c_5 + 7$ are as listed below.

Table 3.34. Equalities 3.34

$c_2 =$	4	6			
$c_3 + 1 =$	4	6			
$c_4 + 5 =$		4	8	10	
$c_5 + 7 =$		4	6	10	

The previous table implies that if $0 * 8 = 2$ and $0 * 6 = 12$. Then $c_2 = 4$ or $c_2 = 6$. If $c_2 = 4$ then we obtain the following table.

Table 3.35. Equalities 3.35

$c_3 + 1 =$		6			
$c_4 + 5 =$				10	
$c_5 + 7 =$			6		

The previous table implies that $c_3 + 1 = c_5 + 7$ which is a contradiction. Therefore if $0 * 8 = 2$ and $0 * 6 = 12$ then $c_2 \neq 4$. Next letting $c_2 = 6$ we obtain the following table.

Table 3.36. Equalities 3.36

$c_3 + 1 =$	4				
$c_4 + 5 =$		4	8		
$c_5 + 7 =$		4		10	

This implies that $c_3 + 1 = 4$. However if $c_3 + 1 = 4$ we loose all choices for $c_4 + 5$ and $c_5 + 7$ and therefore we conclude that if $0 * 8 = 2$ then $0 * 6 \neq 4, 8, 10, 12$. This

implies that $0 * 8 \neq 2$. It is important to reiterate that the proof for any applicable choice for c will lead to the same conclusion. Thus case 1 fails to construct a Cayley table and since the other cases have the same conclusion we conclude that there does not exist a m-inverse loop of order 15 with a long inverse cycle when $(n-1)/2$ is the smallest positive integer such that $[(n-1)/2](3m+1) \equiv 0$. We have proven the following.

Theorem 4. *A 1-inverse loop of order* 15 *with a long inverse cycle does not exist.*

3.3   M-inverse loops of order 3k+2 with a long inverse cycle

In this section we study m-inverse loops of order $n = 3(2k_1+1)+2$ for $k_1 \in Z^+$. The goal of this section is to determine ways to fill out row zero when $n = 3(2k_1+1)+2$. The majority of the work has already been accomplished since most of the propositions in the first section hold true in this section. We will continue the same approach in determining if a m-inverse loop exist of order $3k+2$, by first completing row zero and then examining row one. Let's prove the following propositions that will assist us with our goal.

Proposition 20. *If* $n = 3k+2$ *then* $3(n-1)/2$ *does not divide* $n^2 - 3n + 2 - (n-1)$ *nor* $n^2 - 3n + 2 - (n-1)/2$.

Proof. Assume that $3(n-1)/2$ divides $n^2 - 3n + 2 - (n-1)$ and $n^2 - 3n + 2 - (n-1)/2$ where $n = 3k+2$. This implies that $[3(n-1)/2]k_1 = n^2 - 3n + 2 - (n-1) = [(n-1)(n-2)] - (n-1)$ and $[3(n-1)/2]k_2 = n^2 - 3n + 2 - (n-1)/2 = [(n-1)(n-2)] - (n-1)/2$ for some $k, k_1, k_2 \in Z^+$. Therefore, $(3/2)k_1 = (n-3)$ and $(3/2)k_2 = (n-5/2)$; since $n = 3k+2$ this implies that $3k_1 = 2(3k+2) - 6$ and $3k_2 = 2(3k+1) - 5$. Thus

$2k - k_1 = 2/3$ and $2k - k_2 = 1/3$. However $2k - k_1$ and $2k - k_2 \in Z$. Therefore, $3(n-1)/2$ does not divide $n^2 - 3n + 2 - (n-1)$ nor $n^2 - 3n + 2 - (n-1)/2$.

$\square$

Proposition 21. *If $n = 3k + 2$ then $3(n-1)/2$ divides $(n^2 - 3n + 2)$.*

Proof. Let $n = 3(2k_1 + 1) + 2$; thus $n - 1 = 2(3k_1 + 2)$ and $3(n-1)/2 = 3(3k_1 + 2)$. Consider $(n^2 - 3n + 2) = (n-1)(n-2) = (2(3k_1 + 2))(2(3k_1 + 2) - 1) = 3(3k_1 + 2)(4k_1 + 4)$. Therefore, $3(n-1)/2$ divides $(n^2 - 3n + 2)$.

$\square$

Since we are only investigating cases where $(n-1)/2$ is the smallest positive integer such that $[(n-1)/2](3m+1) \equiv 0$. The following condition must hold. If $(Q, *)$ is a m-inverse loop of order $3k+2$ where $(n-1)/2$ is the smallest positive integer such that $[(n-1)/2](3m+1) \equiv 0$, then for all $a, b, c \in Q$, the choice $a * b = c$ generates $3(n-1)/2$ entries in the Cayley table. Now in order to fill row zero we first determine the amount of missing entries in row zero. Recall that $n = 3k + 2 = 3(2k_1 + 1) + 2$ where $0 * 1 = e$ and $0 * e = 0$ are given. Since we have been given the entry zero then the amount of even missing entries is one less than the amount of odd missing entries. Thus, there are $3k_1 + 2$ odd missing entries and $3k_1 + 1$ even missing entries in row zero.

We define A,B, and C as before. Next we determine the maximum number of equalities that can be used from A in order to complete row zero. Recall that each choice $0 * b = c$ contained in A will only generate 3 odd entries in row zero. Therefore, the maximum number of equalities that can be utilized to complete row zero from A is k_1. Notice we again allow the first form to complete row zero to consist of k_1 equalities from A. The following table shows the number of equalities derived when

$0 * b = c$ is taken from set A, B and B. We designate forms $1 - k_1$ to all possible combinations.

Table 3.37. Completion of row zero for order $3k + 2$

Form	$0 * b = c$ from A	$0 * b = c$ from B	$0 * b = c$ from C
1	k_1	2	$3k_1 - 1$
2	$k_1 - 1$	5	$3k_1 - 4$
3	$k_1 - 2$	8	$3k_1 - 7$
4	$k_1 - 3$	10	$3k_-9$
...	....	.....	
$k_1 - 1$	$k_1 - (k_1 - 2)$	$3(k_1 - 2) + 2$	$3k_1 + 1 - [3(k_1 - 2) + 2]$
k_1	$k_1 - (k_1 - 1)$	$3(k_1 - 1) + 2$	$3k_1 + 1 - [3(k_1 - 1) + 2]$

We conclude that there are k_1 options to complete row zero if using equalities from set A. Next we consider if it is possible to complete row zero with equalities only equalities extracted from set B. We know that the choices $0 * b = c \in A$ and the choices $0 * b = c \in B$ generate the odd entries in row zero. However since we do not want to use equalities from set A then we need $3k_1 + 1$ equalities from set B to fill row zero. Recall that the equalities in set B generate one odd and one even entry in row zero and there are $3k_1 + 2$ odd and $3k_1 + 1$ even missing entries in row zero. Therefore, since the amount of odd missing entries is not equal to the amount of even missing entries. We have that row zero cannot be filled with only equalities from set B. We need a combination from A and B, but these forms are included in the k_1 options. Therefore, there are k_1 ways of selecting equalities from sets A,B, and C to complete row zero.

3.3.1   M-inverse loop of order 11 with a long inverse cycle

Now we apply the information that has been obtained on m-inverse loop of order $n = 3k + 2$, to determine if a m-inverse loop of order $n = 11 = 3(3) + 2$ exists, for some m such that 5 is the smallest positive integer such that $5(3m + 1) \equiv 0$. Assume that $n = 3(3) + 2$ where $Q = e, 0, 1...9$ and $3m + 1 \not\equiv 0$. Again in this section we will use the previous proposition and the help of Mathlab to determine if a m-inverse loop of order 11 with a long inverse cycle exist when $3m + 1 \not\equiv 0$. Now it has been determined that if the order of Q is $3k + 2$ then there are k_1 ways to complete row zero where $3k_1 + 2$ is the number of missing odd entries in row zero. This implies that $k_1 = 1$ since there are 5 odd missing entries. Therefore, there is one way to construct row zero. The unique form used to complete row zero consists of the choice $0 * b = c \in A$, two choices $0 * b = c$ from B and two choices $0 * b = c$ from C.

Recall that if a m-inverse loop of order $3k + 2$ exists where $(n - 1)/2$ is the smallest positive integer such that $[(n - 1)/2](3m + 1) \equiv 0$ then for all $a, b, c \in Q$, the choice $a * b = c$ generates $3(n - 1)/2$ entries in the Cayley table. In our case $n = 11$. Thus the choice $a * b = c$ generates 15 entries in the Cayley table. Now form 1 gives 5 unique equalities, therefore by completing row zero we generate 75 entries in the Cayley table. Let $(Q, *)$ be a m-inverse loop of order 11; we know that 31 of the 121 entries in the Cayley table are given. This implies that 90 entries are missing, thus by completing row zero we obtain 75 of the 90 missing entries.

Next we determine the amount of entries that we obtained in row 1 after row zero was completed. First recall the equalities used to complete row zero. We have the choice $0 * b = c$ from A, two choices $0 * b = c$ from B and two choices $0 * b = c$ from C. Now the choice $0 * b = c$ from A does not generate any entries in row 1, but the 2 equalities from B each generate 1 odd entry in row 1 and the 2 equalities from

C generate 1 odd and 1 even entry in row 1. Therefore, by completing row zero we obtain 4 odd and 2 even entries in row 1. This implies that there are 3 even entries missing in row 1. We know that if row zero is completed and $(n-1)/2$ is the smallest positive integer such that $[(n-1)/2](3m+1) \equiv 0$ then all the odd entries are filled in the Cayley table and the even rows and columns are also filled. We have 75 of the 90 missing entries; therefore we need 15 even entries to complete the Cayley table. This implies that there exist a choice $1 * b = c$ that generates 15 even entries in the Cayley table where 3 of the 15 even entries are in row 1. Therefore, b is odd and c is even.

Next we will determine the appropriate b and c such that $1 * b = c$ generates 3 even entries in row 1. Now it has been previously noted that in order to determine the equalities that hold when the choice $a * b = c$ we can refer to the set X_j for $j = 0, 1..., ((n-1)/2) - 1$. Consider X_j listed below where $a = 1$.

Table 3.38. Iteration 3.38

$[1 + j(3m+1)] * [b + j(3m+1)] = [c + j(3m+1)]$
$[c + j(3m+1) + m] * [1 + j(3m+1) + (m+1)] = [b + j(3m+1) + m]$
$[b + j(3m+1) + 2] * [c + j(3m+1) + (2m+1)] = [1 + j(3m+1) + (2m+1)]$

Now we know that choice $a * b = c$ generates $3(n-1)/2$ entries in the Cayley table. This implies that there are $3(n-1)/2$ unique equalities that must hold if $1 * b = c$. Since each equality is unique, the choice $1 * b = c$ can only appear one time in the iteration for $j = 0, 1..., ((n-1)/2) - 1$. Moreover there cannot exist some b_1 such that $1 * b_1 = c$ since b is the unique element such that $1 * b = c$. Recall that the first term determines what row the entry is inputted in. Therefore the choices are $c + j(3m+1) + m$ and $b + j(3m+1) + 2m$ since each term is congruent to some odd

element of Q when b is odd and c is even for $j = 0, 1..., ((n-1)/2) - 1$. This implies that there are $(n-1)/2$ of these terms. Therefore, for some j, $c+j(3m+1)+m \equiv 1$ and $b+j(3m+1)+2m \equiv 1$. Next assume $c+j(3m+1)+m \equiv 1$ and $1+j(3m+1)+m+1 \equiv b$; this implies that $1*b = c$ appears twice in the iteration and that $1-c \equiv j(3m+1)+m$. Thus $2 - c \equiv j(3m+1)+m+1$ for $j = 0, 1..., ((n-1)/2) - 1$; therefore $b + c \equiv 3$. From here it follows that if $b+c \equiv 3$ then $1*b = c$ will appear twice in the iteration which is a contradiction. Therefore $b + c \not\equiv 3$ which implies that $1*1 \neq 2$, $1*3 \neq 0$, $1*5 \neq 8$, $1*7 \neq 6$, $1*9 \neq 4$.

Next assume for some j, $b+j(3m+1)+2m \equiv 1$ and $c+j(3m+1)+2m+1 \equiv b$. Again this implies that $1*b = c$ appears twice in the iteration and that $1 - b \equiv j(3m+1)+m$; thus $2 - b \equiv j(3m+1)+m+1$ and $2b \equiv c+2$. Hence if $2b \equiv c+2$, then $1*b = c$ will appear twice in the iteration which is a contradiction; therefore $2b \not\equiv c+2$ which implies that $1*1 \neq 0$, $1*3 \neq 4$, $1*5 \neq 8$, $1*7 \neq 2$, $1*9 \neq 6$, since b is odd and c is even.

Finally assume $c + j(3m+1)+m \equiv 1$ and $b+j(3m+1)+m \equiv c$. This implies that there exist $1*b_1 = c$ and that $1-c \equiv j(3m+1)+m$. Thus $c-b \equiv j(3m+1)+m$ and $2c \equiv b+1$. Hence if $2c \equiv b+1$ then there exist $1*b_1 = c$ which is a contradiction since b is the unique element such that $1*b = c$. Therefore $2c \not\equiv b+1$ which implies that $1*1 \neq 6, 1*3 \neq 2$, $1*5 \neq 8$, $1*7 \neq 4$, $1*9 \neq 0$.

Now the choices for c are $0, 2, 4, 6, 8$ since $n = 11$. Therefore the following table displays the possible choices for entries in row one once row zero is filled. Each column, respectively, represent the 3 entries for row one after row zero is filled.

Table 3.39. Equalities 3.39

$1 * 1 = 4$	$1 * 1 = 8$	$1 * 3 = 6$	$1 * 3 = 8$
$1 * 5 = 2$	$1 * 5 = 2$	$1 * 7 = 8$	$1 * 7 = 0$
$1 * 9 = 8$	$1 * 9 = 4$	$1 * 5 = 0$	$1 * 5 = 6$

Observe that if the choice $1 * b = c$ generate 3 even entries in row one after row zero is filled then the entries generated in row one are $2, 4, 8$ or $0, 6, 8$. We used Mathlab to determine the following results: If $(Q, *)$ is a m-inverse of order 11 such that $3m + 1 \not\equiv 0$ and $0 * b = c \in A$ then the choice $0 * b = c$ generates the entries $1, 3, 7$ or $5, 7, 9$ in row zero. Also, if $(Q, *)$ is a m-inverse loop of order 11 such that $3m + 1 \not\equiv 0$ and $1 * b = c$ generates 3 entries in row one after row zero is filled then the choice $1 * b = c$ generates the entries $2, 4, 8$ or $0, 6, 8$ in row one. Therefore if $(Q, *)$ is a m-inverse loop of order 11 then one of the following conditions must hold:

1. The choice $0 * b = c \in A$ generates the entries $1, 3, 7$ in row zero and the choice $1 * x = y$ generate the entries $2, 4, 8$ are in row one.

2. The choice $0 * b = c \in A$ generates the entries $1, 3, 7$ in row zero and the choice $1 * x = y$ generate the entries $0, 6, 8$ are in row one.

3. The choice $0 * b = c \in A$ generates the entries $5, 7, 9$ in row zero and the choice $1 * x = y$ generate the entries $2, 4, 8$ are in row one.

4. The choice $0 * b = c \in A$ generates the entries $5, 7, 9$ in row zero and the choice $1 * x = y$ generate the entries $0, 6, 8$ are in row one.

We will only look at the second condition since the proof of the other conditions is similar and leads to the same conclusion. Recall that the choice $0 * b = c \in B$ generates one odd and one even entry in row zero and the choice $0 * b = c \in C$

generates one odd and one even entry in row one. Assume the choice $0 * b = c \in A$ generates the entries $1, 3, 7$ in row zero and the choice $1 * x = y$ generates the entries $0, 6, 8$ in row one. This implies that there exist two choices $0 * b = c \in B$ that generates the entries 5 and 9 respectively and that there exist two choices $0 * b = c \in C$ that generate the entries 2 and 4 in row one respectively. First we will determine to what value is b congruent to such that the choice $0 * b = c \in B$ generate the entries 5 or 9 in row zero. Then we will determine to what value b is congruent to such that the choice $0 * b = c \in C$ generates 2 or 4 in row one. Since we are again looking for the equalities that hold when the choice $a * b = c$ we will refer to set X_j listed below for $j = 0, 1..., ((n-1)/2) - 1$ where $a = 0$.

Table 3.40. Iteration 3.40

$[0 + j(3m+1)] * [b + j(3m+1)] = [c + j(3m+1)]$
$[c + j(3m+1) + m] * [0 + j(3m+1) + (m+1)] = [b + j(3m+1) + m]$
$[b + j(3m+1) + 2] * [c + j(3m+1) + (2m+1)] = [0 + j(3m+1) + (2m+1)]$

First we determine the choice $0 * b = c$ from B that generates the entry 5 in row zero. Let $0 * b = c$ where b and c are even. Recall that the first term in each equality determines what row the entry will be inputted in. Therefore, $j(3m+1), b + j(3m+1) + 2m$ and $c + j(3m+1) + m$ are the possible choices. Since m is odd this implies $3m + 1$ is even therefore $c + j(3m+1) + m$ is congruent to some odd element of Q; however $j(3m+1)$ and $b + j(3m+1) + 2m$ are congruent to some even element of Q for $j = 0, 1..., ((n-1)/2) - 1$. Recall that $j(3m+1) \equiv 0$ when $j = 0$ which is already represented by the choice $0 * b = c$. Since c is even and $c \not\equiv 5$ we must examine the term $b + j(3m+1) + 2m$, where $b + j(3m+1) + 2m$ is to congruent

to some even element of Q. This implies for some j, $b + j(3m + 1) + 2m \equiv 0$. Now in order for the choice $0 * b = c$ to generate the entry 5 in row zero we must have $0 + j(3m+1) + 2m + 1 \equiv 5$ and $b + j(3m+1) + 2m \equiv 0$. Therefore $j(3m+1) + 2m \equiv 4$ thus $b + 4 \equiv 0$. Thus we conclude that the choice $0 * 6 = c$ generate the entry 5 in row zero and $0 * (c + 5) = 5$. Next we determine the choice $0 * b = c$ from B that generates the entry 9 in row zero. To obtain this information we follow the same steps that we used to find which $0 * b = c$ generates the entry 5 in row zero. Therefore, let $0 + j(3m + 1) + 2m + 1 \equiv 9$ and $b + j(3m + 1) + 2m \equiv 0$; this implies for some j, $0 + j(3m + 1) + 2m \equiv 8$ and $b + 8 \equiv 0$. We conclude that the choice $0 * 2 = c$ generates the entry 9 in row zero and $0 * (c + 9) = 9$.

Next we will identify which $0 * b = c$ from C generates the entry 2 in row 1 with b odd and c even. Again the first term in each equality determines what row the entry will be inputted in; thus $j(3m+1)$, $b + j(3m+1) + 2m$ and $c + j(3m+1) + m$ are the possible choices. However only the terms $b + j(3m+1) + 2m$ and $c + j(3m+1) + m$ are congruent to some odd element of Q. Therefore for some j, $b + j(3m + 1) + 2m \equiv 1$ and $c + j(3m+1) + m \equiv 1$. However only the entry associated with $c + j(3m+1) + m$ generates an even entry in the Cayley table. Therefore letting $c + j(3m + 1) + m \equiv 1$ and $b + j(3m + 1) + m \equiv 2$ we get $1 - c \equiv j(3m + 1) + m$. Therefore, $b + 1 - c \equiv 2$. This implies that $b = c + 1$. We conclude that the choice $0 * (c + 1) = c$ generates the entry 2 in row 1. Finally we determine the choice $0 * b = c \in C$ that generates the entry 4 in row 1. Let $c + j(3m + 1) + m \equiv 1$ and $b + j(3m + 1) + m \equiv 4$; this implies $1 - c \equiv j(3m + 1) + m$ and $b + 1 - c \equiv 4$. Hence $b = c + 3$. Thus we conclude that the choice $0 * (c + 3) = c$ generates the entry 4 in row 1. Therefore, if $(Q, *)$ is a m-inverse loop of order 11 such that the choice $0 * b = c$ from A generates the entries

62

$1, 3, 7$ in row zero and the choice $1 * h = k$ generates the entries $0, 6, 8$ in row one then the following equalities must hold.

Table 3.41. Iteration 3.41

$0 * 6 = c$
$0 * (c + 5) = 5$
$0 * 2 = c_1$
$0 * (c_1 + 9) = 9$
$0 * (c_2 + 1) = c_2$
$0 * (c_3 + 3) = c_3$

Recall that the choice $0 * 6 = c$ and the choice $0 * 2 = c_1$ are from set B and the choice $0 * (c_2 + 1) = c_2$ and $0 * (c_3 + 3) = c_3$ are from set C. Therefore, c, c_1, c_2 and c_3 are even. Now the table below displays the possible choices for an entry in the Cayley table. For example the following table implies that $0 * 6 = c = 2, 4,$ or 8 where 0 and 6 are excluded since $(Q, *)$ is a loop. Note the following table will be used to determine if the above equalities hold.

Table 3.42. Equalities 3.42

$c =$	2	4		8
$c_1 =$		4	6	8
$c_2 =$	2	4	6	8
$c_3 =$	2	4	6	

Case 1a

63

Let $c = 2$; this implies that $0 * 6 = 2$ and $0 * 7 = 5$. Recall c, c_1, c_2 and c_3 are even, so $c_2 + 1$ and $c_3 + 3$ are odd. Therefore, c_1, c_2 and c_3 cannot equal 2. Also note that $c_1 + 9$, $c_2 + 1$ and $c_3 + 3$ cannot be congruent to 7 and that $2 - c_1 \not\equiv 4$. Therefore, we obtain the following table.

Table 3.43. Equalities 3.43

$c_1 =$	4	6			
$c_2 =$		4		8	
$c_3 =$			6		

The previous table implies that $c_3 = 6$. Thus $0 * 9 = 6$. Therefore c_1 and c_2 cannot equal 6 and $c_1 + 9$ and $c_2 + 1$ cannot be congruent to 9. Thus we obtain the following table.

Table 3.44. Equalities 3.44

$c_1 =$	4				
$c_2 =$		4			

This implies $c_1 = c_2$ which is a contradiction since the choices c_1 and c_2 are unique. Hence $0 * 6 \neq 2$.

Case 1b

Let $c = 4$; this implies that $0 * 6 = 4$ and $0 * 9 = 5$. Recall c, c_1, c_2 and c_3 are even. Thus $c_2 + 1$ and $c_3 + 3$ are odd. Therefore, c_1, c_2 and c_3 cannot equal 4. Also,

$c_1 + 9$, $c_2 + 1$ and $c_3 + 3$ cannot be congruent to 9. Also $2 - c_1 \not\equiv 2$. Therefore we obtain the following table.

Table 3.45. Equalities 3.45

$c_1 =$			6	8	
$c_2 =$	2			6	
$c_3 =$	2				

This implies that $c_3 = 2$. Thus $0 * 5 = 2$. Therefore, c_1 and c_2 cannot equal 2. Also $c_1 + 9$ and $c_2 + 1$ cannot be congruent to 5. Therefore we obtain the following table.

Table 3.46. Equalities 3.46

$c_1 =$				8		
$c_2 =$				6		

This implies $c_1 = 8$. Hence $0 * 2 = 8$, $0 * 7 = 9$ and $c_2 = 6$. Thus $0 * 7 = 6$ which is a contradiction. Hence $0 * 6 \neq 4$

Case 1c

Let $c = 8$; this implies that $0 * 6 = 8$ and $0 * 3 = 5$. Recall c, c_1, c_2 and c_3 are even. Thus $c_2 + 1$ and $c_3 + 3$ are odd. Therefore, c_1, c_2 and c_3 cannot equal 8. Also note that $c_1 + 9$, $c_2 + 1$ and $c_3 + 3$ cannot be congruent to 3 and $2 - c_1 \not\equiv 8$. Therefore, we obtain the following table.

Table 3.47. Equalities 3.47

$c_1 =$		6			
$c_2 =$		4	6		
$c_3 =$	2	4	6		

This implies that $c_1 = 6$ and $0 * 5 = 9$. Therefore, c_3 and c_2 cannot equal 6 and $c_1 + 9$ and $c_2 + 1$ cannot be congruent to 5. Therefore, we obtain the following table.

Table 3.48. Equalities 3.48

$c_2 =$					
$c_3 =$		4			

This implies there is no choice for c_2 so $0 * 6 \neq 8$. Furthermore $0 * 6 \neq 2, 4$ or 8. Therefore, there does not exist a m-inverse loop of order 11 when $(n - 1)/2$ is the smallest positive integer such that $[(n - 1)/2](3m + 1)$. We have proven the following:

Theorem 5. *A 1-inverse loop with a long inverse cycle of order 11 does not exist.*

66

CHAPTER 4

The existence of m-inverse quasigroups of order n with a long inverse cycle.

4.1   Introduction to m-inverse quasigroups of order n with a long inverse cycle

In this chapter we investigate the existence of m-inverse quasigroups of order $3k$, $3k+1$, and $3k+2$ with a long inverse cycle that meet the following conditions: m is odd and n is even. Therefore, $gcd(3m+1, n) > 1$ and $n/2$ is the smallest positive integer such that $(n/2)(3m+1) \equiv 0$ where the arithmetic is modulo n. We may suppose without lost of generality that the elements of Q are $0, 1.......n-1$. Also that the notation is chosen such that $J = (0, 1.....n-1)$: that is, so that $(0, 1.....n-1)$ is the long inverse cycle and $J(a) \equiv a+1$. In this chapter we prove the following results: a 3-inverse loop of order 16 with a long inverse cycle exists when $8(3m+1) \equiv 0$, a 7-inverse loop of order 20 with a long inverse cycle exists when $10(3m+1) \equiv 0$, and a 3-inverse loop of order 12 with a long inverse cycle does not exists when $6(3m+1) \equiv 0$. We continue with the same approach that was used when investigating m-inverse loops with a long inverse cycles. First, we determine how many ways row zero can be filled. Then we examine row one to determine if the completion of row one leads to the construction of a Cayley table. Let $(Q, *)$ be a m-inverse quasigroup with a long inverse cycle. Then there exist a permutation J define by $J(a) \equiv a + 1$ such that $[J^m(a * b)] * [J^{m+1}(a)] = J^m(b)$. This implies that the equalities generated by the choice $a * b = c$ are generated in the same manner as m-inverse loops with a long inverse cycle. Thus the following set of equalities hold.

Table 4.1. Iteration 4.1

$a * b = c$
$[c + m] * [a + (m + 1)] = [b + m]$
$[b + 2m] * [c + (2m + 1)] = [a + (2m + 1)]$
$[a + 1(3m + 1)] * [b + 1(3m + 1)] = [c + 1(3m + 1)]$
$[c + 1(3m + 1) + m] * [a + 1(3m + 1) + (m + 1)] = [b + 1(3m + 1) + m]$
$[b + 1(3m + 1) + 2m] * [c + 1(3m + 1) + (2m + 1)] = a + 1(3m + 1) + (2m + 1)]$
$[a + 2(3m + 1)] * [b + 2(3m + 1)] = c + 2(3m + 1)]$
$[c + 2(3m + 1) + m] * [a + 2(3m + 1) + (m + 1)] = b + 2(3m + 1) + m]$
$[b + 2(3m + 1) + 2m] * [c + 2(3m + 1) + (2m + 1)] = [a + 2(3m + 1) + (2m + 1)]$
....
....
$[a + (s - 1)(3m + 1)] * [b + (s - 1)(3m + 1)] = [c + (s - 1)(3m + 1)]$
$[c + (s - 1)(3m + 1) + m] * [a + (s - 1)(3m + 1) + (m + 1)] = [b + (s - 1)(3m + 1) + m]$
$[b + (s - 1)(3m + 1) + 2m] * [c + (s - 1)(3m + 1) + (2m + 1)] = [a + (s - 1)(3m + 1) + (2m + 1)]$
$[a + s(3m + 1)] * [b + s(3m + 1)] = c + s(3m + 1)$

Now as previously shown for m-inverse loops with a long inverse cycle. If the previous set of equalities hold then the following set of the equalities must also hold. Each equality generated by the choice $a * b = c$ can be represented by one of the equalities in X_j.

Table 4.2. X_j

$[a + j(3m + 1)] * [b + j(3m + 1)] = [c + j(3m + 1)]$
$[c + j(3m + 1) + m] * [a + j(3m + 1) + (m + 1)] = [b + j(3m + 1) + m]$
$[b + j(3m + 1) + 2m] * [c + j(3m + 1) + (2m + 1)] = [a + j(3m + 1) + (2m + 1)]$

4.2 M-inverse quasigroups of order $3k + 1$ with a long inverse cycle.

In this section we begin by investigating m-inverse quasigroups with long inverse cycle of order $3k + 1$. The goal of this section is to determine ways to fill out row zero when $n = 3(2k_1 + 1) + 1$ for $k_1 \in Z^+$. Recall that each equality generated by the choice $a * b = c$ can be represented by one of the equalities in X_j for $j = 0, 1, ..., s - 1$ where s is the smallest positive integer such that $s(3m + 1) \equiv 0$. Therefore, the proof for each proposition below is identical to the corresponding propositions associated with m-inverse loops with a long inverse cycle.

Proposition 22. *If $(Q, *)$ is a m-inverse quasigroup of order n with a long inverse cycle then there exist some $t \in Z^+$ such that $t(3m + 1) \equiv 0$.*

Proposition 23. *Let $(Q, *)$ be a m-inverse quasigroup of order n with a long inverse such that $a * b = c$ and $i \neq j$. Then $i(3m + 1) \not\equiv j(3m + 1)$.*

Lemma 4. *If $(Q, *)$ is a m-inverse quasigroup of order n then $a * b = c$ generates $3s$ or s entries in the Cayley table; where s is the smallest positive integer such that $s(3m + 1) \equiv 0$. Note $s = n/2$ for m-inverse quasigroups.*

Proposition 24. *Let $(Q, *)$ be a m-inverse quasigroup of order n with a long inverse cycle.*

1. If $0 * b = c$ generates $3s$ entries in the Cayley table with b even and c odd then the choice $0 * b = c$ generates 3 odd entries in row zero.

2. If $0 * b = c$ generates $3s$ entries in the Cayley table such that b and c are even then the choice $0 * b = c$ generates one odd and one even entry in row zero.

3. If $0 * b = c$ generates $3s$ entries in the Cayley table with b odd and c even then the choice $0 * b = c$ generates one even entry in row zero.

Proposition 25. *Let* $(Q, *)$ *be a m-inverse quasigroup of order n with a long inverse cycle with b even, c odd and the choice* $0 * b = c$ *generates* $3(n/2)$ *entries in the Cayley table. Then the choice* $0 * b = c$ *generates no entries in row one.*

Proposition 26. *Let* $(Q, *)$ *be a m-inverse quasigroup of order n with a long inverse cycle such that b and c are even, and the choice* $0 * b = c$ *generates* $3(n/2)$ *entries in the Cayley table. Then the choice* $0 * b = c$ *generates one odd entry in row one.*

Proposition 27. *Let* $(Q, *)$ *be a m-inverse quasigroup of order n with a long inverse cycle with b odd, c even, and the choice* $0 * b = c$ *generates* $3(n/2)$ *entries in the Cayley table. Then the choice* $0 * b = c$ *generates one odd and one even entry in row one.*

Proposition 28. *Let* $(Q, *)$ *be a m-inverse quasigroup of order n where* $(n)/2$ *is the smallest positive integer such that* $[(n)/2](3m + 1) \equiv 0$ *and row zero is filled. Then all the even rows and columns are filled where only even entries remain unfilled in the odd columns and rows.*

Proposition 29. *Let* $(Q, *)$ *be a m-inverse quasigroup of order n with a long inverse cycle.*

1. If $0 * b = c \in B$ *and* $0 * b_1 = c_1 \in B$ *then* $b - c \not\equiv b_1 - c_1$.

2. If $0 * b = c \in C$ *and* $0 * b_1 = c_1 \in C$ *then* $b - c \not\equiv b_1 - c_1$.

Now the following propositions must be proving since the proofs are not the same as when investigating m-inverse loops with a long inverse cycle.

Proposition 30. *If* $(Q, *)$ *is a quasigroup of order* $n = 3k + 1$ *with a long inverse cycle, then* $a * [a + 2(k_1(3m + 1) + 2m + 1)] = a + k_1(3m + 1) + 2m + 1$ *generates* $n/2$ *entries in the Cayley table for* $k, k_1 \in Z^+$.

Proof. Assume the choice $a * b = c$ generates $(n)/2$ entries in the Cayley table. Recall from the previous proposition that $s \equiv 3j + 1$ or $s \equiv 3j + 2$ for $j = 0, 1, ..., s - 1$. Recall that $s = n/2$. This implies that $s = 3k_1 + 2$. Therefore $j \equiv k_1$ which implies that the choice $a * b = c$ is equivalent to the third equality in the table below.

Table 4.3. Iteration 4.3

$[a + (3j)m + (i)] * [b + (3j)m + (i)] = [c + (3j)m + (j)]$
$[c + (3j + 1)m + (j)] * [a + (3j + 1)m + (j) + 1] = [b + (3j) + 1)m + (j)]$
$[b + (3j + 2)m + (j)] * [c + (3j + 2)m + (j) + 1] = [a + (3j + 2)m + j + 1]$

Therefore $b \equiv +2j(3m + 1) + 2m + 1)$ and $c \equiv a + j(3m + 1) + 2m + 1$. However since $k_1 \equiv j$. Thus we conclude $a * [a + 2k_1(3m + 1) + 2m + 1)] = a + k_1(3m + 1) + 2m + 1$ generates $n/2$ distinct entries in the Cayley table. $\square$

Proposition 31. *If $n = 3k + 1$ for some $k \in Z^+$ then $3(n/2)$ divides $(n^2 - n)$*

Proof. Let $n = 3(2k_1 + 1) + 1 = 2(3k_1 + 2)$; this implies that $3(n/2) = 3(3k_1 + 2)$ where $k_1 \in Z^+$. Consider $(n^2 - n) = [2(3k_1 + 2)][2(3k_1 + 2)] - 2(3k_1 + 2) = 3(3k_1 + 2)(4k_1 + 2)$. Therefore $3(n/2)$ divides $(n^2 - n)$.

$\square$

Proposition 32. *If $n = 3k + 1$, for some $k \in Z^+$ then $3(n/2)$ does not divide n^2 nor $n^2 - (n/2)$*

Proof. Assume $n^2 = [(3/2)n]k_1$ and $n^2 - (n)/2 = [(3/2)n]k_2$ for some $k, k_1, k_2 \in Z^+$. This implies that $n = (3/2)k_1$ and $(n - 1/2) = (3/2)k_2$. Since $n = 3k + 1$ then $3k + 1 = (3/2)k_1$ and $3k + 1 = (3/2)k_2 + (1/2)$. Therefore $k_1 - 2k = 2/3$ and

$k_2 - 2k = (1/3)$. Thus both equalities leads to a contradiction since $k, k_1, k_2 \in Z^+$. Thus $3(n/2)$ does not divide n^2 nor $n^2 - (n/2)$.

$\square$

Let's use the previous propositions to determine ways to fill out row zero for a m-inverse quasigroup of order $3k + 1$ with a long inverse cycle. Once a particular manner for completing row zero is determined, the next objective is to determine what entries in row one are missing. Once this information is obtained we decide if the completion of row one leads to the construction of a Cayley table. In order to determine how many possible ways we can fill row zero we must determine the number of missing entries in row zero where the missing entries are characterized as odd or even. Now the order of Q is $n = 3(2k_1 + 1) + 1$. Therefore, there are $3k_1 + 2$ odd and $3k_1 + 2$ even entries in row zero. Recall that the choice $0 * b = c$ generates either three odd entries in row zero, one even one odd even entry in row zero or one even entry in row zero. Let's again define A,B,C as previously noted. Next we determine the maximum amount of equalities that can be used from A in order to complete row zero. By proposition 30, we need the choice $a * b = c$ and the choice $a_1 * b_1 = c_1$ which generates $n/2$ entries in the Cayley table respectively. Therefore, since $a * [a + 2(k_1(3m + 1) + 2m + 1)] = a + k_1(3m + 1) + 2m + 1$ generates $n/2$ entries in the Cayley table then $0 * [0 + 2(k_1(3m + 1) + 2m + 1)] = 0 + k_1(3m + 1) + 2m + 1$ and $1 * [1 + 2(k_1(3m + 1) + 2m + 1)] = 1 + k_1(3m + 1) + 2m + 1$. This implies that there are $3k_1 + 1$ odd missing entries in row one. Now each choice $0 * b = c$ from A generate 3 odd entries in row zero. Therefore, k_1 is the maximum amount of equalities that can be utilized from A to complete row zero. The following table shows the number of equalities derived when $0 * b = c$ is taken from set A, B and B. We designate forms $1 - k_1$ to all possible combinations.

Table 4.4. Completion of row zero for order $3k + 1$

Form	$0 * b = c \in A$	$0 * b = c \in C$	$0 * b = c \in A$
1	k_1	1	$(3k_1 + 2) - 1$
2	$k_1 - 1$	4	$(3k_1 + 2) - 4$
3	$k_1 - 2$	7	$(3k_1 + 2) - 7$
...	....	....	
k_1	$k_1 - (k_1 - 1)$	$3(k_1 - 1) + 1$	$(3k_1 + 2) - 3(k_1 - 1) + 1$

Next we consider if it is possible to fill row zero with equalities that are not extracted from set A. In view of the fact that there are $3k_1 + 1$ odd and $3k_1 + 2$ even missing entries in row zero we conclude that we need at least one choice from set A to fill out row zero. Therefore, there are k_1 possible ways of selecting equalities from set A,B and C.

4.2.1 3-inverse quasigroups of order 16 with a long inverse cycle

In this section we apply the results from the previous section to prove the following theorem.

Theorem 6. *A 3-inverse quasigroup with a long inverse cycle of order 16 exists.*

Proof. Let $n = 16 = 3(5) + 1$ and $m = 3$. This implies that $2k_1 + 1 = 5$. Thus $k_1 = 2$. Therefore, there are three ways to complete row 1. Next we will use form 2 to complete row zero. Therefore we must have one equality $0 * b = c \in A$, four equalities $0 * b = c \in B$ and four equalities $0 * b = c \in C$. We also need the choice $a * b = c$ and the choice $a_1 * b_1 = c_1$ that generates $n/2$ entries in the Cayley table respectively. Let $0 * 6 = 11$, $1 * 7 = 12$, $0 * 0 = 3 \in A$, $0 * 2 = 6 \in B$,$0 * 8 = 4 \in B$,$0 * 10 = 0 \in B$, $0 * 12 = 10 \in B$, and $0 * 1 = 2 \in C$, $0 * 3 = 14 \in C$, $0 * 9 = 12 \in C$ and

$0 * 11 = 8 \in C$ which leads us to following Cayley table. Thus a 3-inverse quasiqroup of order 16 with a long inverse cycle exist. The table below gives the Cayley table for such structure.

Table 4.5. 3-inverse quasigroup of order 16 with a long inverse cycle

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	3	2	6	14	1	15	11	7	4	12	0	8	10	9	13	5
1	0	8	11	1	6	9	14	12	3	2	4	10	13	15	5	7
2	15	7	5	4	8	0	3	1	13	9	6	14	2	10	12	11
3	7	9	2	10	13	3	8	11	0	14	5	4	6	12	15	1
4	14	13	1	9	7	6	10	2	5	3	15	11	8	0	4	12
5	1	3	9	11	4	12	15	5	10	13	2	0	7	6	8	14
6	6	14	0	15	3	11	9	8	12	4	7	5	1	13	10	2
7	10	0	3	5	11	13	6	14	1	7	12	15	4	2	9	8
8	12	4	8	0	2	1	5	13	11	10	14	6	9	7	3	15
9	11	10	12	2	5	7	13	15	8	0	3	9	14	1	6	4
10	5	1	14	6	10	2	4	3	7	15	13	12	0	8	11	9
11	8	6	13	12	14	4	7	9	15	1	10	2	5	11	0	3
12	13	11	7	3	0	8	12	4	6	5	9	1	15	14	2	10
13	2	5	10	8	15	14	0	6	9	11	1	3	12	4	7	13
14	4	12	15	13	9	5	2	10	14	6	8	7	11	3	1	0
15	9	15	4	7	12	10	1	0	2	8	11	13	3	5	14	6

□

4.3   M-inverse quasigroups of order $3k + 2$ with a long inverse cycle

In this section we investigate the existence of m-inverse quasigroups with a long inverse cycle of order $3k + 2$. The goal of this section is to determine ways to fill out row zero when $n = 3(2k_1) + 2$ for $k_1 \in Z^+$. Note that proposition 1.1-12.1 still hold.

Next we introduce the following propositions to assist us with the investigation of m-inverse quasigroups of order $3k + 2$ with a long inverse cycle.

Proposition 33. *If $(Q, *)$ is a m-inverse quasigroup with a long inverse cycle of order $n = 3k + 2 = 3(2k_1) + 2$ for some $k_1 \in Z^+$ then $a * [a + k_1(3m + 1) + m + 1] = a + 2k_1(3m + 1) + 2m + 1$ generates $(n/2)$ distinct entries in the Cayley table.*

Proof. Assume the choice $a * b = c$ generates $(n)/2$ entries in the Cayley table. Recall from the previous proposition that $s \equiv 3j + 1$ or $s \equiv 3j + 2$ and $s = (n)/2$. This implies that $s = 3k_1 + 1$. Therefore $k_1 \equiv j$ which implies that $a * b = c$ is equivalent to the second equality in the table below.

Table 4.6. Iteration 4.6

$[a + (3j)m + (i)] * [b + (3j)m + (i)] = [c + (3j)m + (j)]$
$[c + (3j + 1)m + (j)] * [a + (3j + 1)m + (j) + 1] = [b + (3j) + 1)m + (j)]$
$[b + (3j + 2)m + (j)] * [c + (3j + 2)m + (j) + 1] = [a + (3j + 2)m + j + 1]$

Therefore $b \equiv a + j(3m+1) + m + 1$ and $c \equiv a + 2j(3m+1) = 2m + 1$. However $k_1 \equiv j$. Thus we conclude that $a * a + k_1(3m + 1) + m + 1 = a + 2k_1(3m + 1) + 2m + 1$ generates $(n)/2$ entries in the Cayley table.

$\square$

Proposition 34. *If $n = 3k + 2$ for some $k \in Z^+$ then $3(n/2)$ divides $(n^2 - n/2)$*

Proof. Let $n = 3(2k_1) + 2 = 2(3k_1 + 1)$; this implies that $3(n/2) = 3(3k_1 + 1)$ where $k_1 \in Z^+$. Consider $(n^2 - n/2) = [2(3k_1+1)][2(3k_1+1)] - (3k_1+1) = 3(3k_1+1)(4k_1+1)$. Therefore $3(n/2)$ divides $(n^2 - n/2)$. $\square$

Proposition 35. *If $n = 3k + 2$ for some $k \in Z^+$ then $3(n/2)$ does not divide n^2 nor $n^2 - n$.*

Proof. Assume $n^2 = [(3/2)n]k_1$ and $n^2 - n = [(3/2)n]k_2$ for some $k, k_1, k_2 \in Z^+$. This implies that $n = (3/2)k_1$ and $n - 1 = (3/2)k_2$. Thus $3k + 2 = (3/2)k_1$ and $3k + 1 = (3/2)k_2$. Therefore $k_1 - 2k = 4/3$ and $k_2 - 2k = (2/3)$. Thus both equalities leads to a contradiction since $k, k_1, k_2 \in Z^+$. This implies that $3(n/2)$ does not divide n^2 nor $n^2 - n$.

$\square$

Let $n = 3(2k_1) + 2$ for some $k_1 \in Z^+$. This implies that there are $3k_1 + 1$ odd entries and $3k_1 + 1$ even entries in row zero. Notice by propositions 34 and 35 that in order for a m-inverse loop of order $3k + 2$ to exist there must exist some choice $a * b = c$ that generates $n/2$ entries in the Cayley table. Let $k_0 = k_1(3m + 1) + m$. This implies that $0 * (k_0 + 1) = 2k_0 + 1$ or $1 * [1 + (k_0 + 1)] = 1 + (2k_0 + 1)$. Now we determine the possible ways to complete row zero. We do this by determining the maximum amount of equalities from set A that can be used to fill row zero. Since there are $3k_1 + 1$ odd entries in row zero then the maximum amount of equalities is k_1. The following table shows the number of equalities derived when $0 * b = c$ is taken from set A, B and B. We designate forms $1 - 2k_1$ to all possible combinations.

Table 4.7. Completion of row zero for order $3k + 2$

Form	$0 * b = c \in A$	$0 * b = c \in C$	$0 * b = c \in C$
1	k_1	0	$3k_1 + 1$
2	k_1	1	$(3k_1 + 1) - 1$
3	$k_1 - 1$	3	$(3k_1 + 1) - 3$
4	$k_1 - 1$	4	$(3k_1 + 1) - 4$
...	......	....	....
$2k_{-1}$	$k_1 - (k_1 - 1)$	$3(k_1 - 1)$	$(3k_1 + 1) - (3(k_1 - 1))$
$2k_1$	$k_1 - (k_1 - 1)$	$3(k_1 - 1) + 1$	$(3k_1 + 2) - 3(k_1 - 1) + 1$

76

Note that the previous table only displays the forms that consist of the choices $0 * b = c \in A$. However if $1 * [1 + (k_0 + 1)] = 1 + (2k_0 + 1)$ then there are $3k_1 + 1$ odd and $3k_1 + 1$ even missing entries. Hence the final form consists of $3k_1 + 1$ equalities $0 * b = c \in B$. Therefore, there are $2k_1 + 1$ possible ways to complete row zero.

4.3.1   7-inverse quasigroups of order 20 with a long inverse cycle

In this section we apply the results from the previous section to prove the following theorem.

Theorem 7. *A 7-inverse quasigroup with a long inverse cycle of order 20 exists.*

Proof. Since $n = 20 = 3(6) + 2$ and $m = 7$ then we have $2k_1 = 6$. Therefore, there are 7 possible ways to select equalities for set A,B and C to complete row zero. Let's use form $2k_1$ from table 4.6 to complete row zero. This implies that we need one equality $0 * b = c \in A$, seven equalities $0 * b = c \in B$ and three equalities $0 * b = c \in C$. Also we need the choice $a * b = c$ that generates $n/2$ entries in the Cayley table. Therefore, if we choose $0 * 0 = 3 \in A$, $0 * 2 = 2 \in B$, $0 * 6 = 4 \in B$, $0 * 8 = 10 \in B$, $0 * 10 = 6 \in B$, $0 * 12 = 18 \in B$, $0 * 14 = 8 \in B$, $0 * 16 = 0 \in B$, $0 * 9 = 14 \in C$, $0 * 11 = 12 \in C$ and $0 * 13 = 16 \in C$. These choices leads us to the following Cayley table. Thus a 7-inverse quasiqroup of order 20 with a long inverse cycle exists.

Table 4.8. 7-inverse quasigroup of order 20 with a long inverse cycle

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	3	19	2	13	1	5	4	9	10	14	6	12	18	16	8	7	0	11	17	15
1	1	10	17	11	15	9	18	13	16	4	0	2	19	12	7	8	5	14	3	6
2	19	17	5	1	4	15	3	7	6	11	12	16	8	14	0	18	10	9	2	13
3	5	8	3	12	19	13	17	11	0	15	18	6	2	4	1	14	9	10	7	16
4	4	15	1	19	7	3	6	17	5	9	8	13	14	18	10	16	2	0	12	1 1
5	9	18	7	10	5	14	1	15	19	13	2	17	0	8	4	6	3	16	11	1 2
6	14	13	6	17	3	1	9	5	8	19	7	11	10	15	16	0	12	18	4	2
7	13	14	11	0	9	12	7	16	3	17	1	15	4	19	2	10	6	8	5	18
8	6	4	16	15	8	19	5	3	11	7	10	1	9	13	12	17	18	2	14	0
9	7	0	15	16	13	2	11	14	9	18	5	19	3	17	6	1	4	12	8	10
10	16	2	8	6	18	17	10	1	7	5	13	9	12	3	11	15	14	19	0	4
11	10	12	9	2	17	18	15	4	13	16	11	0	7	1	5	19	8	3	6	14
12	2	6	18	4	10	8	0	19	12	3	9	7	15	11	14	5	13	17	16	1
13	8	16	12	14	11	4	19	0	17	6	15	18	13	2	9	3	7	1	10	5
14	18	3	4	8	0	6	12	10	2	1	14	5	11	9	17	13	16	7	15	19
15	12	7	10	18	14	16	13	6	1	2	19	8	17	0	15	4	11	5	9	3
16	17	1	0	5	6	10	2	8	14	12	4	3	16	7	13	11	19	15	18	9
17	11	5	14	9	12	0	16	18	15	8	3	4	1	10	19	2	17	6	13	7
18	0	11	19	3	2	7	8	12	4	10	16	14	6	5	18	9	15	13	1	17
19	15	9	13	7	16	11	14	2	18	0	17	10	5	6	3	12	1	4	19	8

□

4.4 M-inverse quasigroups of order $3k$ with a long inverse cycle

In this section we investigate the existence of m-inverse quasigroups with a long inverse cycle of order $3k$. The goal of this section is to determine ways to fill out row zero when $n = 3(2k_1)$ for $k_1 \in Z^+$. Let's introduce the following propositions to assist us with the investigation of m-inverse quasigroups of order $3k$ with a long inverse cycle.

Proposition 36. *If $n = 3k$ for some $k \in Z^+$ then $3(n/2)$ does not divide $[n^2 - n]$ nor $[n^2 - (n/2)]$.*

Proof. Assume that $n^2 - n = [(3/2)n]k_1$ and $n^2 - n/2 = [(3/2)n]k_2$ for some $k, k_1, k_2 \in Z^+$. This implies that $n - 1 = (3/2)k_1$ and $n - 1/2 = (3/2)k_2$. Since $n = 3k$ then $3k = (3/2)k_1 + 1$ and $3k = (3/2)k_2 + (1/2)$. Therefore $2k - k_1 = 2/3$ and $2k - k_2 = (1/3)$. Thus both equalities leads to a contradiction since $k, k_1, k_2 \in Z^+$. This implies that $3(n/2)$ does not divide $[(n^2 - n)]$ nor $[n^2 - (n/2)]$.

$\square$

Proposition 37. *If $n = 3k$ for some $k \in Z^+$ then $3(n/2)$ divides n^2.*

Proof. Let $n = 3(2k_1)$ $k_1 \in Z^+$; this implies that $3(n/2) = 3(3k_1)$ and $n^2 = (3(2k_1))(3(2k_1)) = 3(3k_1)(4k_1)$. Therefore, $3(n/2)$ divides n^2.

$\square$

Next we assume that $(Q, *)$ is a m-inverse quasigroup of order order $3(2k_1)$ with a long inverse cycle. Therefore, there are $3k_1$ even and $3k_1$ odd missing entries in each row. Also we are not given any entries in the Cayley table therefore there are n^2 missing entries. Recall that the set A contains all the choices $0 * b = c$ that generates three odd entries in row zero. Therefore, the maximum amount of equalities that can be used from set A is again k_1. Also from propositions 36 and 37 we discover that each choice $a * b = c$ must generate $3(n/2)$ entries in the Cayley table. The following table shows the number of equalities derived where $0 * b = c$ is taken from set A, B and B. We designate forms $1 - k_1$ to all possible combinations.

Table 4.9. Completion of row zero for order $3k$

Form	$0 * b = c \in A$	$0 * b = c \in C$	$0 * b = c \in A$
1	k_1	0	$3k_1$
2	$k_1 - 1$	3	$(3k_1 - 3$
3	$k_1 - 2$	6	$(3k_1 - 6$
...	....	....	
k_1	$k_1 - (k_1 - 1)$	$3(k_1 - 1)$	$(3k_1 - 3(k_1 - 1)$

79

Note that the previous table displays the equalities derived where $0 * b = c$ is taken from set A, B and C. Since there are $3k_1$ odd and $3k_1$ even missing entries. We also have the form that consist of $3k_1$ choices $0 * b = c \in B$. Therefore, there are $k_1 + 1$ possible ways of selecting equalities from set A,B and C.

4.4.1   3-inverse quasigroups of order 12 with a long inverse cycle

In this section we apply the results from the previous section to prove the following theorem.

Theorem 8. *A 3-inverse quasigroup with a long inverse cycle of order 12 does not exists.*

Proof. Let $n = 12$. This implies that the arithmetic is modulo 12; also $m = 3$ and $Q = \{0, 1, ...11\}$. Let's assume by way of contradiction that a 3-inverse quasigroup of order 12 with a long inverse cycle exists. Therefore, we need 144 entries to complete the Cayley table and each row is missing six odds and six even entries. Note that if we choose $0 * b = c \in A$ then the choice $0 * b = c$ generates one of the following sets of entries in row zero: $\{1, 3, 9\}$, $\{1, 5, 7\}$ or $\{5, 9, 11\}$. Also note that if the choice $0 * b = c$ generates the entries $\{1, 3, 9\}$ or $\{1, 5, 7\}$ in row zero then $b = 0$. If the choice $1 * h = k$ where h is odd, generates three entries in row one then the choice $1 * h = k$ generates the entries $\{2, 4, 10\}$, $\{2, 6, 8\ \}$ or $\{0, 6, 10\}$ in row one. Note that if the choice $1 * h = k$ generates the entries $\{2, 4, 10\}$ or $\{2, 6, 8\}$ in row one then $h = 1$.

Recapping, $n = 3(4)$ where $k_1 = 2$. This implies there are 3 forms that can be used to fill row zero. Let's consider the first form which consist of two choices $0 * b = c \in A$ and six choices $0 * b = c \in C$. However this form will not lead to the construction of a Cayley table since the choices $0 * b = c \in A$ generates $1, 3, 9$ or

$5, 9, 11$. Since these sets are not disjoint it is impossible to have two choices from set A. Next Let's consider form $k_1 + 1$ which consist of six choices $0 * b = c \in C$. Recall that each choice $0 * b = c \in B$ generates $3(n/2) = 18$ entries in the Cayley table and one odd entry in row one. This implies that by filling row zero we obtain 108 of 144 missing entries for the Cayley table where 6 of the 108 entries are odd entries in row one. Therefore, there are 36 even entries missing in the Cayley table 6 of which are missing for row one. Recall that each choice $a * b = c$ generates 18 entries in the Cayley table. This implies that in order to complete the Cayley table we need two choices $1 * h = k$ the generates three even entries respectively in row one. Note that h is odd since we have established that after row zero is filled all the even columns are also filled. However if the choice $1 * h = k$ generates 18 entries in the Cayley table where h is odd then $1 * h = k$ generates the entries $2, 4, 10$, $2, 6, 8$ or $0, 6, 10$ in row one. Notice that these sets are not disjoint. Therefore, it is impossible to have two equalities $1 * h = k$ that generates 3 entries in row one after row zero is filled. Let's consider form 2 which consists of one equality $0 * b = c \in C$, three equalities $0 * b = c \in B$ and three equalities $0 * b = c \in C$. This implies that after row zero is filled we obtain 126 of 144 missing entries for the Cayley table. Now each choice $0 * b = c \in B$ generates one odd entry in row one. The choice $0 * b = c \in C$ generates one odd entry and one even entry in row one. Therefore 9 of 126 entries are inputted in row one where 6 are odd and 3 are even. Thus, we need three odd entries to fill row one. This leads us to the following 9 cases to determine if form 2 leads to the construction of a Cayley table.

1. Let the choice $0 * b = c \in A$ generate the entries $1, 3, 9$ in row zero and the choice $1 * x = y$ generate the entries $2, 4, 10$ in row one. Note x is odd and y is even.

2. Let the choice $0 * b = c \in A$ generate the entries $1, 3, 9$ in row zero and the choice $1 * x = y$ generate the entries $2, 6, 8$ in row one.

3. Let the choice $0 * b = c \in A$ generate the entries $1, 3, 9$ in row zero and the choice $1 * x = y$ generate the entries $0, 6, 10$ in row one. 4. Let the choice $0 * b = c \in A$ generate the entries $1, 5, 7$ in row zero and the choice $1 * x = y$ generate the entries $2, 4, 10$ in row one.

5. Let the choice $0 * b = c \in A$ generate the entries $1, 5, 7$ in row zero and the choice $1 * x = y$ generate the entries $2, 6, 8$ in row one.

6. Let the choice $0 * b = c \in A$ generate the entries $1, 5, 7$ in row zero and the choice $1 * x = y$ generate the entries $0, 6, 10$ in row one.

7. Let the choice $0 * b = c \in A$ generate the entries $5, 9, 11$ in row zero and the choice $1 * x = y$ generate the entries $2, 4, 10$ in row one.

8. Let the choice $0 * b = c \in A$ generate the entries $5, 9, 11$ in row zero and the choice $1 * x = y$ generate the entries $2, 6, 8$ in row one.

9.Let the choice $0 * b = c \in A$ generate the entries $5, 9, 11$ in row zero and the choice $1 * x = y$ generate the entries $0, 6, 10$ in row one.

We only show case 1 since all other cases are handled similarly and lead to the same conclusion.

Assume $0 * b = c \in A$ generates the entries $1, 3, 9$ in row zero and $1 * x = y$ generates the entries $2, 4, 10$ in row one. This implies that the choice $0 * b = c \in B$ must generate the entry $5, 7$ or 11 in row zero. The choice $0 * b = c \in C$ must generate the entry $0, 6$ or 8 in row one. Next we determine the value to which b is congruent

to when the choice $0 * b = c$ generates the entry 5, 7 or 11 in row zero. Consider the following table:

Table 4.10. Iteration 4.10

$$[a + j(3m + 1)] * [b + j(3m + 1)] = [c + j(3m + 1)]$$
$$[c + j(3m + 1) + m] * [a + j(3m + 1) + (m + 1)] = [b + j(3m + 1) + m]$$
$$[b + j(3m + 1) + 2m] * [c + j(3m + 1) + (2m + 1)] = [a + j(3m + 1) + (2m + 1)]$$

First we determine to which value b is congruent to when the choice $0 * b = c \in B$ generates the entry 5 in row zero. Now in order to generate the entry 5 in row zero we must have $[b + j(3m + 1) + 2m] \equiv 0$ and $[a + j(3m + 1) + (2m + 1)] \equiv 5$. Since $m = 3$ and $a = 0$ then $b + 10j + 6 \equiv 0$ and $10j + 7 \equiv 5$. Therefore $b + 4 \equiv 0$. Thus $b \equiv 8$. We then determine to which value b is congruent to when the choice $0 * b = c \in B$ generates the entry 7 in row zero. This implies $b + 10j + 6 \equiv 0$ and $10j + 7 \equiv 7$. Therefore $b + 6 \equiv 0$. Thus $b \equiv 6$. Lastly we determine to which value b is congruent to when the choice $0 * b = c \in B$ generates the entry 11 in row zero. This implies $b + 10j + 6 \equiv 0$ and $10j + 7 \equiv 11$. Therefore $b + 10 \equiv 0$. Thus $b \equiv 2$. Now from the previous statements the choice $0 * 8 = c$ generates the entry 5 in row zero since $0 * c + 5 = 5$. The choice $0 * 6 = c_1$ generates the entry 7 in row zero since $0 * c_1 + 7 = 7$. And the choice $0 * 2 = c_2$ generates the entry 11 in row zero since $0 * c_2 + 11 = 11$.

Now we determine to which value c is congruent to when the $0 * b = c \in C$ generates the entry $0, 6$, or 8 in row one. First we determine to which value c is congruent to when the choice $0 * b = c \in C$ generates the entry 0 in row one. This implies that $c + 10j + 3 \equiv 1$ and $b + 10j + 3 \equiv 0$. Therefore, $c \equiv b + 1$. Next we

83

determine to which value c is congruent to when the choice $0 * b = c \in C$ generates the entry 6 in row one. This implies that $c + 10j + 3 \equiv 1$ and $b + 10j + 3 \equiv 6$. Therefore, $c \equiv b + 7$. Finally we determine to which value c is congruent to when the choice $0 * b = c \in C$ generates the entry 8 in row one. This implies that $c + 10j + 3 \equiv 1$ and $b + 10j + 3 \equiv 8$. Therefore, $c \equiv b + 5$. Thus the choice $0 * c_3 = c_3 + 1$ generates the entry 0 in row one, the choice $0 * c_4 = c_4 + 7$ generates the entry 6 in row one, and the choice $0 * c_5 = c_5 + 5$ generates the entry 8 in row one. Therefore if $(Q, *)$ is a 3-inverse quasigroup of order 12 such that the choice $0 * b = c$ generates the entries $1, 3, 9$ in row zero and the choice $1 * x = y$ generates the entry $0, 6$ or 8 in row one then the following set of equalities must hold.

Table 4.11. Iteration 4.11

$0 * 8 = c$
$0 * c + 5 = 5$
$0 * 6 = c_1$
$0 * c_1 + 7 = 7$
$0 * 2 = c_2$
$0 * c_2 + 11 = 11$
$0 * c_3 = c_3 + 1$
$0 * c_4 = c_4 + 7$
$0 * c_5 = c_5 + 5$

Note that the proof for any applicable value of c where $0 * 8 = c$ is similar to the proof that will be given below. Therefore we will only show the case when $c = 2$. The goal of this proof is to determine if the previous equalities hold can we construct a Cayley table associated with Q. Recall that $0 * 8 = c$, $0 * 6 = c_1$, and $0 * 2 = c_2$ are from set B and $0 * c_3 = c_3 + 1$, $0 * c_4 = c_4 + 7$, $0 * c_5 = c_5 + 5$ are from set C.

84

Therefore, c, c_1, c_2, $c_3 + 1$, $c_4 + 7$, and $c_5 + 5$ are even and c_i are odd for $i = 3, 4, 5$.

Now the table below displays the possible choices for an entry in the Cayley table .

For example since $0 * 8 = c$ then the table shows that $0 * 8 = c = 0, 2, 4, 6, 8$ or 10.

Table 4.12. Equalities 4.12

$c =$	0	2	4	6	8	10
$c_1 =$	0	2	4	6	8	10
$c_2 =$	0	2	4	6	8	10
$c_3 + 1 =$	0	2	4	6	8	10
$c_4 + 7 =$	0	2	4	6	8	10
$c_5 + 5 =$	0	2	4	6	8	10

Let $c = 2$; this implies that $0 * 8 = 2$ and $0 * 7 = 5$. Recall that c, c_1, c_2, $c_3 + 1$, $c_4 + 5$, and $c_5 + 7$ are even and c_i are odd for $i = 3, 4, 5$. Therefore, c_1, c_2, $c_3 + 1$, $c_4 + 5$, $c_5 + 5$ cannot equal 2; and $c_i \not\equiv 7$ for $i = 3, 4, 5$. Thus $c_1 \not\equiv 0$, $c_2 \not\equiv 8$, $c_3 + 1 \not\equiv 8$, $c_4 + 7 \not\equiv 2$ and $c_5 + 5 \not\equiv 0$. Moreover $6 - c_1 \not\equiv$ and $2 - c_2 \not\equiv 8 - 2$ since $0 * 8 = c$, $0 * 6 = c_1$, and $0 * 2 = c_2$ are from set B. Therefore, the remaining choices for c_2, $c_3 + 1$, $c_4 + 5$, and $c_5 + 7$ are listed below.

Table 4.13. Equalities 4.13

$c_1 =$			4	6	8	10
$c_2 =$	0		4	6		10
$c_3 + 1 =$	0		4	6		10
$c_4 + 7 =$	0			6	8	10
$c_5 + 5 =$			4	6	8	10

Notice from the previous table if $0*8 = 2$ then $0*6 = 4$, $0*6 = 6$, $0*6 = 8$ and $0*6 = 10$.

Case 1a

Let $0*6 = 4$; this implies that $0*11 = 7$. Therefore c_2, $c_3 + 1$, $c_4 + 7$ and $c_5 + 5$ cannot equal to 4. Also c_i cannot be congruent to 11 for $i = 3, 4, 5$ and $2 - c_2 \not\equiv 2$. Therefore, the remaining choices for c_2, $c_3 + 1$, $c_4 + 5$, and $c_5 + 7$ are as listed below.

Table 4.14. Equalities 4.14

$c_2 =$				6		10
$c_3 + 1 =$				6		10
$c_4 + 7 =$	0				8	10
$c_5 + 5 =$				6	8	10

Observe that if $0*8 = 2$ and $0*6 = 4$ then $c_2 = 6$ or $c_2 = 10$. Let $c_2 = 6$. This implies that $0*5 = 11$ and $0*5 = 7$. However if $0*5 = 7$ then $0*5 \neq 7$. Let $c_6 = 10$. This implies that $0*5 = 6$ and $0*5 = 0$. However if $0*5 = 6$ then $0*5 \neq 0$. Thus $0*6 \neq 4$.

Case 1b

Next let $c_1 = 6$; this implies that $0*6 = 6$ and $0*1 = 7$. Therefore we obtain the following table.

Table 4.15. Equalities 4.15

$c_2 =$	0	4			10
$c_3 + 1 =$	0	4			10
$c_4 + 7 =$	0				10
$c_5 + 5 =$		4		8	10

The choices for $c_4 + 7 = 0$ or $c_4 + 7 = 10$. Let $c_4 + 7 = 0$. This implies $0 * 2 = 4$ or $0 * 2 = 10$. Let $0 * 2 = 4$. This implies that $0 * 3 = 11$, and $0 * 3 = 8$. If $0 * 3 = 11$ then $0 * 3 \neq 8$. Therefore $0 * 2 \neq 4$. Let $0 * 2 = 10$. This implies that $0 * 3 = 4$ and $0 * 3 = 8$. If $0 * 3 = 8$ then $0 * 3 \neq 4$. Therefore $0 * 2 \neq 10$. Thus we conclude that $c_4 + 7 \neq 0$. Let $c_4 + 7 = 10$. This implies $0 * 2 = 4$ or $0 * 2 = 0$. Let $0 * 2 = 4$. This implies that $0 * 3 = 11$ and $0 * 3 = 10$. If $0 * 3 = 10$ then $0 * 3 \neq 11$. Therefore $0 * 2 \neq 4$. Let $0 * 2 = 0$. This implies that $0 * 3 = 10$ and $0 * 3 = 4$. If $0 * 3 = 4$ then $0 * 3 \neq 10$. Therefore $0 * 2 \neq 0$. Thus we conclude that $0 * 6 \neq 6$.

Case 1c

Next let $c_1 = 8$. This implies that $0 * 6 = 8$ and $0 * 3 = 7$. Therefore we obtain the following table.

Table 4.16. Equalities 4.16

$c_2 =$	0			6		10
$c_3 + 1 =$	0			6		10
$c_4 + 7 =$	0			6		
$c_5 + 5 =$			4	6		10

87

Notice that the choices for $c_4 + 7$ are 0 and 6. Let $c_4 + 7 = 0$. This implies that $0 * 2 = 6$ or $0 * 2 = 10$. Let $0 * 2 = 6$. This implies that $0 * 5 = 0$ and $0 * 5 = 11$ which is a contradiction. Therefore $0 * 2 \neq 6$. If $0 * 2 = 10$ then we get $0 * 5 = 0$ and $0 * 5 = 6$ which is again a contradiction. Therefore $0 * 2 \neq 10$. Thus we conclude that $c_4 + 7 \neq 0$. Let $c_4 + 7 = 6$. This implies that $0 * 2 = 0$ or $0 * 2 = 10$. Let $0 * 2 = 0$. This leads to the contradictory statements $0 * 11 = 11$ and $0 * 11 = 6$. Therefore $0 * 2 \neq 0$. Let $0 * 2 = 10$. the choice again leads to contradictory statements $0 * 11 = 6$ and $0 * 11 = 0$. Therefore $0 * 2 \neq 10$. Thus we conclude that $c_4 + 7 \neq 6$. Hence both choices for $c_4 + 7$ leads to a contradiction. Therefore $0 * 6 \neq 8$.

Case 1d

Next let $c_1 = 10$; this implies that $0 * 6 = 10$ and $0 * 5 = 7$. Therefore we obtain the following table.

Table 4.17. Equalities 4.17

$c_2 =$	0	4			
$c_3 + 1 =$	0	4			
$c_4 + 7 =$			6	8	
$c_5 + 5 =$		4	6	8	

Notice the choices for c_2 are 0 and 4. Let $c_2 = 0$. This implies that $0 * 2 = 0$. Therefore $0 * 11 = 11$, $0 * 3 = 4$ and $c_4 + 7 = 6$ or $c_4 + 7 = 8$. Let $c_4 + 7 = 6$. This implies that $0 * 11 = 6$. If $0 * 11 = 6$ and $0 * 11 \neq 11$. Thus $c_4 + 7 \neq 6$. Let $c_4 + 7 = 8$. This implies that $0 * 11 = 6$. If $0 * 11 = 6$ then $0 * 11 \neq 11$. Thus $c_4 + 7 \neq 8$. Therefore, we conclude that $c_2 \neq 0$. Let $c_2 = 4$ This implies that $0 * 2 = 4$. Therefore $0 * 3 = 11$, $0 * 11 = 0$ and $c_4 + 7 = 6$ or $c_4 + 7 = 8$. Let $c_4 + 7 = 6$. This implies that

88

$0 * 11 = 6$. However $0 * 11 \neq 0$ if $0 * 11 = 6$. Thus $c_4 + 7 \neq 6$. Let $c_4 + 7 = 8$. This implies that $0 * 11 = 6$. If $0 * 11 = 6$ then $0 * 11 \neq 0$. Thus $c_4 + 7 \neq 8$. Therefore, we conclude that $c_2 \neq 4$. Furthermore $0 * 6 \neq 10$. In conclusion, since $0 * 6 \neq 4$, $0 * 6 \neq 6$, $0 * 6 \neq 8$ or $0 * 6 \neq 10$. This implies that $0 * 8 \neq 2$. Since the proof for each case and any applicable choice for $0 * 8 = c$ lead to a contradiction we conclude that a 3-inverse quasigroup of order 12 with a long inverse cycle does not exist when $(n/2)(3m + 1) \equiv 0$.

$\square$

CHAPTER 5

Conclusion

5.1 Conclusion

Finite inverse loops and quasigroups with long inverse cycles have applications in cryptography as shown by Keedwell.[3] The existence of such structures for some specific orders has been studied extensively by Keedwell[3] and Scherbacov.[5] With our research we continued the investigation of the possible orders for which such structures exist.

In Chapter 2 we started our study by looking at order 9 loops with a long inverse cycle, as well as the quasigroups of order 8 with a long inverse cycle. More specifically we studied the existence of the following algebraic structures: (i) 3 and 7- inverse loops with a long inverse cycle of order 9, and (ii) 3 and 7 inverse quasigroups with a long inverse cycle of order 8. We approached our investigation of such structures by looking at which products $0 * b = c$ would lead to the construction of a Cayley table. After providing the basic definition of m-inverse loops and quasigroups we proved the following.

Theorem 1. A 3 or 7- inverse loop with a long inverse cycle does not exist.

Theorem 2. A 3 or 7- inverse quasigroup with a long inverse cycle does not exist.

In Chapters 3 and 4 we generalized the work from Chapter 2 to order $3k$, $3k+1$ and $3k + 2$. More specifically in Chapter 3 we studied the existence of m-inverse loops with a long inverse cycle of order $3k$ and $3k + 2$. Notice the existence for order

3k + 1 was studied by Keedwell in.[1] We showed the different ways to fill out row zero for each particular order and after this information was provided we proved the following:

Theorem 3. A 1-inverse loop with a long inverse cycle of order 11 does not exist.

Theorem 4. A 1-inverse loop with a long inverse cycle of order 15 does not exist.

In chapter 4 we studied the existence of m-inverse quasigroups with a long inverse cycle of order $3k$, $3k + 1$ and $3k + 2$. We again showed the different ways to fill out row zero for each particular order and after this information was provided we proved the following:

Theorem 5. A 3-inverse quasigroup with a long inverse cycle of order 16 exists.

Theorem 6. A 7-inverse quasigroup with a long inverse cycle of order 20 exists.

Theorem 7. A 3-inverse quasigroup with a long inverse cycle of order 12 does not exist.

Notice that our work, together with previous work of Keedwell, completely answers the question of the existence of finite m-inverse loops and quasigroups with a long inverse cycle for all orders.

REFERENCES

[1] A. D. Keedwell and V. A. Shcherbacov (2002), On m-inverse loops and quasi-groups with a long inverse cycle, Australas. J. Combin. 26, 99-119.

[2] R. Artzy, On loops with a special property, Proc. Amer. Math. Soc. 6(1955), 448-453.

[3] A.D. Keedwell, Crossed-inverse quasigroups with long inverse cycles and applications to cryptography, Australas. J. Combin. 20(1999), 241-250.

[4] A.D. Keedwell, Construction, properties and applications of finite neofields, Comment. Math. Univ. Carolinae 41(2000), 283-297.

[5] V.A. Shcherbacov, Quasigroups in cryptology, Computer Science Journal of Moldova, vol.17, no. 2(50), 2009, 193-228

BIOGRAPHICAL STATEMENT

Carl E. Looney was born in Garland, Texas, in 1978. He received his B.S. degree in mathematics from University of Texas at Arlington in 2009. From 2009 to 2015 he worked as a graduate teaching assistant for the University of Texas at Arlington while pursing his Ph.d in mathematics. He was reared by Carl and Maurene Looney. He has eight wonderful supportive siblings.