On m-inverse loops and quasigroups with a long inverse cycle

A. D. Keedwell

Department of Mathematics and Statistics
University of Surrey
Guildford GU2 7XH
Surrey, United Kingdom

V. A. Shcherbacov

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
MD-2028 Chisinau
Moldova

Abstract

In an earlier paper, we showed that CI-loops and quasigroups with long inverse cycles have certain properties which make them particularly appropriate for use in cryptography. The same is true of the generalized structures called m-inverse loops and quasigroups. Here, we investigate the existence of such structures (initially for small orders).

I. Introduction

A *finite quasigroup* $(Q, \circ)$ of order n consists of a set Q of symbols on which a binary operation $(\circ)$ is defined such that (i) for all pairs of elements $a, b \in Q$, $a \circ b \in Q$ (*closure*) and (ii) for all pairs $a, b \in Q$, there exist unique elements $x, y \in Q$ such that $x \circ a = b$ and $a \circ y = b$ (*unique solubility of equations*).

If there exists an element $e \in Q$ such that, for all $a \in Q$, $e \circ a = a = a \circ e$ (*existence of a two-sided identity element*), the quasigroup is a *loop*.

A quasigroup may satisfy some or all of the following inverse properties:

(i) for each $a \in Q$, there exists an element $a_L^{-1} \in Q$ such that $a_L^{-1} \circ (a \circ b) = b$ for all $b \in Q$ (*the left inverse property*);

(ii) for each $a \in Q$, there exists an element $a_R^{-1} \in Q$ such that $(b \circ a) \circ a_R^{-1} = b$ for all $b \in Q$ (*the right inverse property*);

(iii) for each $a \in Q$, there exists an element $a'_L \in Q$ such that $a'_L \mathrm{o} (b \circ a) = b$ for all $b \in Q$ (*the left crossed-inverse property*);

(iv) for each $a \in Q$, there exists an element $a'_R \in Q$ such that $(a \circ b) \circ a'_R = b$ for all $b \in Q$ (*the right crossed-inverse property*).

A quasigroup which satisfies (i) and (ii) is called an *inverse-property quasigroup*. One which satisfies (iii) and (iv) is called a *crossed-inverse-property quasigroup* (or, for brevity, a *CI-quasigroup*). For a quasigroup which is commutative, (i)$\Leftrightarrow$(iii) and (ii)$\Leftrightarrow$(iv) so the inverse and crossed inverse properties coincide.

A quasigroup or loop $(Q, \circ)$ of finite order which has the left crossed-inverse property also has the right crossed-inverse property; and conversely. So a quasigroup which has either one of these properties is a CI-quasigroup. For such a quasigroup, the mapping J: $a \to a'_R$ is a permutation of the elements of Q. (For a proof of these remarks, see Lemma 1.1 of [4].)

In [3], Karklinüsh and Karklin have generalized the concept of a CI-loop to what they have called an m-inverse loop. We can generalize the concept of a CI-quasigroup in a similar way as follows:

Suppose that there exists a permutation J of the elements of a quasigroup $(Q, \circ)$ such that, for all $a, b \in Q, (a \circ b)J^m \circ aJ^{m+1} = bJ^m$. Then $(Q, \circ)$ is an *m-inverse quasigroup*. In particular, a CI-quasigroup is a 0-inverse quasigroup. When the permutation J is written in the form of a product of cycles, these cycles are called the *inverse cycles* of the m-inverse quasigroup.

By an *m-inverse loop* $(L, \circ)$ we shall mean an m-inverse quasigroup with identity element e such that $eJ = e$. Then, putting $b = e$ in the relation $(a \circ b)J^m \circ aJ^{m+1} = bJ^m$, we find that $aJ^m \circ aJ^{m+1} = e$ for all elements $a \in L$. Let b be an arbitrary element of the loop. Then there exists an element $a \in L$ such that $aJ^m = b$. But, $aJ^m \circ aJ^{m+1} = e$. That is, $b \circ bJ = e$ for all $b \in L$. (This agrees with the definition given in [3].)

In [4], it was shown that CI-quasigroups with long inverse cycles have a role to play in cryptography and the same is true of m-inverse loops and quasigroups. The purpose of the present paper is to determine for which orders m-inverse loops and quasigroups with a long inverse cycle exist.

We first investigate the existence of m-inverse loops. Since every loop of order less than five is a group, we need only consider loops of orders $n \geq 5$.

R. Artzy[1] has shown that 0-inverse loops of order $n > 3$ with an inverse cycle of length $n - 1$ do not exist so an m-inverse loop $(m > 0)$ which has such a maximal length cycle cannot satisfy the crossed-inverse property. We say that an m-inverse loop which is not also an $(m - 1)$-inverse loop is *proper* so, in particular, a 1-inverse loop which has a single long inverse cycle of length $n - 1$ must be proper.

II. The existence of proper m-inverse loops with a long inverse cycle, $m \geq 1$

We may suppose without loss of generality that the elements of Q are $e, 0, 1, \ldots, n-2$, where e is the identity element, and that the notation is chosen so that $J = (e)(0\ 1\ \cdots\ n-2)$: that is, so that $(0\ 1\ \cdots\ n-2)$ is the long inverse cycle. Then

$aJ \equiv a+1 \mod (n-1)$ for $a \in \{0,1,\ldots,n-2\}$ and $eJ = e$. Also, $a \circ aJ = e$: that is, $a \circ (a+1) \equiv e \mod (n-1)$.

For $a,b,c \neq e$, $a \circ b = c \Rightarrow (a-m)J^m \circ [b-(m+1)]J^{m+1} = (c-m)J^m$.

But, $([b-(m+1)] \circ (c-m))J^m \circ [b-(m+1)]J^{m+1} = (c-m)J^m$ by the m-inverse property. So, $[b-(m+1)] \circ (c-m) = a-m$. Iterating this result, we have $a \circ b = c \Rightarrow [b-(m+1)] \circ (c-m) = a-m \Rightarrow [c-(2m+1)] \circ (a-2m) = b-(2m+1) \Rightarrow [a-(3m+1)] \circ [(b-(3m+1)] = [c-(3m+1)]$.

Thus, J^{3m+1} is an automorphism. In fact, J^{3m+1} is an automorphism of any m-inverse loop, as was first pointed out in [3].

For an m-inverse loop of order $(3m+1)+1$, the relation $[a-(3m+1)] \circ [(b-(3m+1)] = [c-(3m+1)]$ is equivalent to $a \circ b = c$ since, in such a loop, arithmetic of elements is modulo $3m+1$. (The 1-inverse loops of order 5 and the 2-inverse loops of order 8 exhibited later in this paper are examples.)

For an m-inverse loop of order n, where $n-1$ is relatively prime to $3m+1$, the implication $a \circ b = c \Rightarrow [a-(3m+1)] \circ [(b-(3m+1)] = [c-(3m+1)]$ leads to the implication $a \circ b = c \Rightarrow (a+h) \circ (b+h) = (c+h)$ for all integers h because there exist integers r, s such that $r(n-1) - s(3m+1) = 1$ and so $-s(3m+1) \equiv 1 \mod (n-1)$ whence $a - s(3m+1) \equiv a+1$, $b - s(3m+1) \equiv b+1$, $c - s(3m+1) \equiv c+1$. By iteration, the result follows. Thus, in this case, J itself is an automorphism of the loop. It also follows that such a loop is $(m+l)$-inverse for all positive integers l.

Lemma 2.1 *In an m-inverse loop (with a long inverse cycle) of order n, where $n-1$ is relatively prime to $3m+1$, $0 \circ h = k$ (for $h,k \neq e$) implies that $0 \circ (k-h+1) = (n-h)$ and that $0 \circ (n-k) = (h-k)$.*

Proof. $0 \circ h = k \Rightarrow [h-(m+1)] \circ (k-m) = (n-1)-m \mod (n-1) \Rightarrow 0 \circ (k-h+1) = (n-h)$ by adding $m+1-h$ to each element. That is, $0 \circ h = k \Rightarrow 0 \circ h_1 = k_1$, where $h_1 = k-h+1$ and $k_1 = n-h$. Iterating this implication yields the desired result. (Note that $h_3 \equiv h \mod (n-1)$ and that $k_3 \equiv k$.)

Corollary 2.2 *When $n-1$ is relatively prime to $3m+1$ in an m-inverse loop of order n with a long inverse cycle, $0 \circ 2 = v$ is always impossible for $v = 1$ and is impossible for $v = 3$ unless $n = 5$.*

Proof. $0 \circ 2 = v \Rightarrow 0 \circ (v-1) = n-2$ and $0 \circ (n-v) = n+1-v \mod (n-1)$ by the Lemma. So, when $v = 1$, we have $0 \circ 2 = 1 \Rightarrow 0o0 = n-2$ and $0 \circ (n-1) = n$ or $0 \circ 0 = 1$. The equalities $0 \circ 2 = 1$ and $0 \circ 0 = 1$ are contradictory. When $v = 3$, we have $0 \circ 2 = 3 \Rightarrow 0 \circ 2 = n-2$ and $0 \circ (n-3) = n-2$. These are mutually contradictory except when $n = 5$.

(a) m-inverse loops of order 5 with an inverse cycle of length 4.

Here, $Q = \{e,0,1,2,3\}$ and $J = (e)(0\ 1\ 2\ 3)$. Suppose that $0 \circ 2 = v$. Then $v \neq 0,2$ and, since $0 \circ 1 = e$, $v \neq e$.

When $3m+1$ is relatively prime to four, $v = 1$ is impossible by Corollary 2.2 so $v = 3$ is the only possibility. This case occurs only when $m = 2$ in the present situation since an $(m+4)$-inverse loop is an m-inverse loop because J^4 is the identity mapping.

In fact, proper m-inverse loops of order five with $m > 1$ do not exist, as we shall show. However, there exist four isomorphically distinct proper 1-inverse loops of order five. We may show this as follows:

Putting $0 \circ 0 = u$ and using the relation $a \circ b = c \Rightarrow (b-2) \circ (c-1) \equiv (a-1) \bmod 4$, we find that $2 \circ (u+3) = 3$ and that $(u+1) \circ 2 = 1$. Clearly, $u \neq 0$ or e since these two elements already occur elsewhere in row 0 of the Cayley table of the loop. (See Figure 2a.1.)

$(\circ)$	e	0	1	2	3
e	e	0	1	2	3
0	0	u	e	$\cdot$	$\cdot$
1	1	$\cdot$	$\cdot$	e	$\cdot$
2	2	$\cdot$	$\cdot$	$\cdot$	e
3	3	e	$\cdot$	$\cdot$	$\cdot$

Fig. 2a.1.

We find that the remaining values of u define proper 1-inverse loops as follows:

Try $u = 1$. Then $2 \circ 0 = 3$ and $2 \circ 2 = 1$. The Cayley table is uniquely completable as is shown in Figure 2a.2. (The integer superscripts indicate one order in which the cells may be filled.) To check that the table gives a 1-inverse loop, we require the following relations to hold:

$0 \circ 1 = e; 1 \circ 2 = e; 2 \circ 3 = e$; and $3 \circ 0 = e$
$0 \circ 2 = 3 \Rightarrow 0 \circ 2 = 3$
$0 \circ 3 = 2 \Rightarrow 1 \circ 1 = 3 \Rightarrow 3 \circ 2 = 0 \Rightarrow 0 \circ 3 = 2$
$1 \circ 0 = 2 \Rightarrow 2 \circ 1 = 0 \Rightarrow 3 \circ 3 = 1 \Rightarrow 1 \circ 0 = 2$
$1 \circ 3 = 0 \Rightarrow 1 \circ 3 = 0$
$2 \circ 0 = 3 \Rightarrow 2 \circ 2 = 1 \Rightarrow 0 \circ 0 = 1 \Rightarrow 2 \circ 0 = 3$
$3 \circ 1 = 2 \Rightarrow 3 \circ 1 = 2$

$(\circ)$	e	0	1	2	3
e	e	0	1	2	3
0	0	1	e	3^9	2^8
1	1	2^4	3^3	e	0^5
2	2	3	0^1	1	e
3	3	e	2^2	0^6	1^7

Fig. 2a.2.

So the table defines a proper 1-inverse loop of order five. [We may easily check that it is not a 0-inverse loop. For example, $(2 \circ 2) \circ 2J = 1 \circ 3 = 0 \neq 2$.]

Try $u = 3$. Then $2 \circ 2 = 3$ and $0 \circ 2 = 1$. The Cayley table is uniquely completable as is shown in Figure 2a.3. To check that the table gives a 1-inverse loop, we require the following relations to hold:

$0 \circ 1 = e; 1 \circ 2 = e; 2 \circ 3 = e$; and $3 \circ 0 = e$
$0 \circ 2 = 1 \Rightarrow 0 \circ 0 = 3 \Rightarrow 2 \circ 2 = 3 \Rightarrow 0 \circ 2 = 1$
$0 \circ 3 = 2 \Rightarrow 1 \circ 1 = 3 \Rightarrow 3 \circ 2 = 0 \Rightarrow 0 \circ 3 = 2$
$1 \circ 0 = 2 \Rightarrow 2 \circ 1 = 0 \Rightarrow 3 \circ 3 = 1 \Rightarrow 1 \circ 0 = 2$
$1 \circ 3 = 0 \Rightarrow 1 \circ 3 = 0$
$2 \circ 0 = 1 \Rightarrow 2 \circ 0 = 1$
$3 \circ 1 = 2 \Rightarrow 3 \circ 1 = 2$

$(\circ)$	e	0	1	2	3
e	e	0	1	2	3
0	0	3	e	1	2^9
1	1	2^4	3^5	e	0^8
2	2	1^2	0^3	3	e
3	3	e	2^6	0^1	1^7

Fig. 2a.3.

So the table defines a proper 1-inverse loop of order five.

Try $u = 2$. Then $2 \circ 1 = 3$ and $3 \circ 2 = 1$. The Cayley table completes uniquely to the partial form shown in Figure 2a.4. This has two completions. We need to check whether either completed table represents a 1-inverse loop. In fact, we find that both completed tables represent proper 1-inverse loops of order five with a long inverse cycle.

In particular, $1 \circ 1 = 0 \Rightarrow 3 \circ 3 = 0 \Rightarrow 1 \circ 3 = 2 \Rightarrow 1 \circ 1 = 0$ and $3 \circ 1 = 2 \Rightarrow 3 \circ 1 = 2$. On the other hand, $1 \circ 1 = 2 \Rightarrow 3 \circ 1 = 0 \Rightarrow 3 \circ 3 = 2 \Rightarrow 1 \circ 1 = 2$ and $1 \circ 3 = 0 \Rightarrow 1 \circ 3 = 0$.

$(\circ)$	e	0	1	2	3
e	e	0	1	2	3
0	0	2	e	3^1	1^2
1	1	3^4	$\cdot$	e	$\cdot$
2	2	1^3	3^5	0^6	e
3	3	e	$\cdot$	1^7	$\cdot$

Fig. 2a.4.

We conclude that, up to isomorphism, there exist just four distinct proper 1-inverse loops of order five with a long inverse cycle.

As regards the existence of 2-inverse or 3-inverse loops, we have $0 \circ 0 = u \Rightarrow 1 \circ (u-2) = 2 \Rightarrow (u-1) \circ 0 = 3$ for a 2-inverse loop. If $u = 1$, $0 \circ 0 = 1 \Rightarrow 0 \circ 0 = 3$. If $u = 2$, $0 \circ 0 = 2 \Rightarrow 1 \circ 0 = 2$. If $u = 3$, $0 \circ 0 = 3 \Rightarrow 2 \circ 0 = 3$. Each of these implications is contradictory.

For a 3-inverse loop, $0 \circ 0 = u \Rightarrow -4 \circ (u-3) = -3 \Rightarrow (u-7) \circ (-2) = -3$. That is, $0 \circ 0 = u \Rightarrow 0 \circ (u+1) = 1 \Rightarrow (u+1) \circ 2 = 1$. If $u = 1$, $0 \circ 0 = 1 \Rightarrow 0 \circ 2 = 1$. If $u = 3$, $0 \circ 0 = 3 \Rightarrow 0 \circ 0 = 1$. Each of these is contradictory. If $u = 2$, $0 \circ 0 = 2 \Rightarrow 0 \circ 3 = 1$ and $3 \circ 2 = 1$. We find that we obtain the partial Cayley table given in Figure 2a.4. However, $1 \circ 1 = 0 \Rightarrow -3 \circ -3 = -2$ or $1 \circ 1 = 2$ and $1 \circ 1 = 2 \Rightarrow -3 \circ -1 = -2$ or $1 \circ 3 = 2$. Both are contradictory.

(b) *m*-inverse loops of order 6 with an inverse cycle of length 5.

We assume that $J = (e)(0\ 1\ 2\ \cdots\ 4)$ and that $0 \circ 2 = v$, $v \neq 0, 2$ or e as usual. Arithmetic is modulo 5.

When $n - 1 = 5$ is relatively prime to $3m + 1$: that is, when $m \neq 5h + 3$, $0 \circ (v-1) = 4$ and $0 \circ (6-v) = 2 - v$ by Lemma 2.1. Also, J is an automorphism of the loop.

We have $v \neq 1$ or 3 by Corollary 2.2. If $v = 4$, the equalities $0 \circ 2 = v$ and $0 \circ (v-1) = 4$ contradict each other. Thus, no 1, 2 or 4-inverse loops of order 6 with a long inverse cycle exist.

For a 3-inverse loop, the automorphism J^{10} is the identity because J^5 is the identity. We have $a \circ b = c \Rightarrow (b-4) \circ (c-3) = (a-3) \Rightarrow (c-2) \circ (a-1) = (b-2) \Rightarrow a \circ b = c$ so, in general, an entry c in cell (a, b) determines the entries in two other cells. However, $a \circ (a-1) = (a+2) \Rightarrow a \circ (a-1) = (a-3)$. Since $a + 2 \Rightarrow a - 3$

mod 5, an entry $a+2$ in cell $(a, a-1)$ determines no others. All together, there are $20 = (6\times 3)+2$ cells to be filled so just two of the cells of type $(a, a-1)$ must contain $a+2$. An example of a 3-inverse loop for which $0 \circ 2 = 1$ is given in Figure 2b.1.

$(\circ)$	e	0	1	2	3	4
e	e	0	1	2	3	4
0	0	3	e	1	4	**2**
1	1	2	4	e	0	3
2	2	4	3	0	e	1
3	3	1	0	4	2	e
4	4	e	2	3	**1**	0

$0 \circ 2 = 1 \Rightarrow 3 \circ 3 = 2 \Rightarrow 4 \circ 4 = 0$
$0 \circ 0 = 3 \Rightarrow 1 \circ 0 = 2 \Rightarrow 1 \circ 4 = 3$
$0 \circ 3 = 4 \Rightarrow 4 \circ 1 = 2 \Rightarrow 2 \circ 4 = 1$
$1 \circ 3 = 0 \Rightarrow 4 \circ 2 = 3 \Rightarrow 3 \circ 0 = 1$
$1 \circ 1 = 4 \Rightarrow 2 \circ 1 = 3 \Rightarrow 2 \circ 0 = 4$
$2 \circ 2 = 0 \Rightarrow 3 \circ 2 = 4 \Rightarrow 3 \circ 1 = 0$
$0 \circ 4 = 2; 4 \circ 3 = 1$

Fig. 2b.1.

(c) m-inverse loops of order 7 with an inverse cycle of length 6.

No such loops exist. We have the following more general theorem:

Theorem 2.3 *m-inverse loops of order $n = 3l+1$ with an inverse cycle of length $3l$ do not exist.*

Proof. We assume that $J = (e)(0\ 1\ 2\ \cdots\ 3l-1)$ so that arithmetic is modulo $3l$.

In this case, $n-1 = 3l$ is relatively prime to $3m+1$ for all values of m, so $0 \circ h = k \Rightarrow 0 \circ (k-h+1) = (n-h) \Rightarrow 0 \circ (n-k) = (h-k)$ by Lemma 2.1. Also, J is an automorphism of the loop.

Let us consider row 0 of the Cayley table of the loop. In this row, the cells $(0, e)$ and $(0, 1)$ are already filled with the elements 0 and e respectively. So $n-2 = 3l-1$ cells remain to be filled. But, putting the entry k in cell $(0, h)$ forces the entries $n-h = 3l+1-h$ and $h-k$ in the cells $(0, k-h+1)$ and $(0, n-k)$ respectively. Moreover, the three cells $(0, h)$, $(0, k-h+1)$ and $(0, n-k)$ are distinct for all choices of h and k. We may show this as follows:

The first two coincide only if $k-h+1 \equiv h$ and $(3l+1-h) \equiv k \mod 3l$. The first and last coincide only if $(3l+1)-k \equiv h$ and $h-k \equiv k \mod 3l$. Each of these pairs of equalities requires that $3h \equiv 2$ and $3k \equiv 1 \mod 3l$. Both the latter congruences are impossible.

Since there are $3l-1$ cells to be filled in row 0 and this is not a multiple of three, the Cayley table cannot be completed.

(d) m-inverse loops of order 8 with an inverse cycle of length 7.

We assume that $J = (e)(0\ 1\ 2\ \cdots\ 6)$ and that $0 \circ 2 = v$, $v \neq 0, 2$ or e. Arithmetic is modulo 7.

When $n-1 = 7$ is relatively prime to $3m+1$, $0 \circ (v-1) = 6$ and $0 \circ (8-v) = 2-v$ by Lemma 2.1. Also, J is an automorphism of the loop. Since $0 \circ (v-1) = 6$, $v \neq 3$ or 6 otherwise $0 \circ 2 = v$ and $0 \circ (v-1) = 6$ are mutually contradictory. Furthermore, $v \neq 1$ by Corollary 2.2. Thus, $v \neq 0, 1, 2, 3, 6$ or e.

If $v = 4$, $0 \circ 2 = 4$, $0 \circ 3 = 6$ and $0 \circ 4 = 5 (\equiv -2)$. Because J is an automorphism of the loop, $a \circ b = c \Rightarrow (a+h) \circ (b+h) = (c+h)$ and so the entries of the left-to-right

broken diagonals headed by $0 \circ 2 = 4$, $0 \circ 3 = 6$ and $0 \circ 4 = 5$ in the Cayley table of the loop are all determined. In particular, $5 \circ 0 = 2$, $4 \circ 0 = 3$ and $3 \circ 0 = 1$. Then no element for $0 \circ 0$ exists (as is shown in Figure 2d.1) so the table cannot be completed.

If $v = 5$, we have $0 \circ 2 = 5$, $0 \circ 4 = 6$ and $0 \circ 3 = 4 (\equiv -3)$, whence $5 \circ 0 = 3$, $3 \circ 0 = 2$ and $4 \circ 0 = 1$. We again find that no element for $0 \circ 0$ exists so the table cannot be completed.

$(\circ)$	e	0	1	2	3	4	5	6
e	e	0	1	2	3	4	5	6
0	0	(?)	e	4	6	5	·	·
1	1	·	·	e	5	0	6	·
2	2	·	·	·	e	6	1	0
3	3	1	·	·	0	e	0	2
4	4	3	2	·	·	1	e	1
5	5	2	4	3	·	·	2	e
6	6	e	3	5	4	·	·	·

Fig. 2d.1.

Thus, no m-inverse loop of order 8 with a long inverse cycle of length 7 exists when $3m + 1$ is relatively prime to 7. However, existence when $m = 7h + 2 (\equiv 2 \mod 7)$ is possible. Let us consider, in more detail, 2-inverse loops of order 8.

We have $J = (e)(0\ 1\ 2\ 3\ 4\ 5\ 6)$. Then $a \circ (a+1) = e$. Also, $a \circ b = c$

$$\Rightarrow (b-3) \circ (c-2) = (a-2) \Rightarrow (c-5) \circ (a-4) = (b-5) \Rightarrow (a-7) \circ (b-7) = (c-7)$$

which is equivalent to $a \circ b = c$ since addition is modulo 7. Thus, in general, each relation $a \circ b = c$ implies two others. Therefore, putting entry c in cell (a, b) forces two other entries. However, $a \circ (a+3) = a+5 \Rightarrow a \circ (a+3) = a-2$. Since $a - 2 \equiv a + 5 \mod 7$, it is permissible to put the entry $a + 5$ in the cell $(a, a + 3)$ without contradiction but such an entry forces no others.

$(\circ)$	e	0	1	2	3	4	5	6
e	e	0	1	2	3	4	5	6
0	0	1	e	3	**5**	2	6	4
1	1	5	4	e	0	**6**	2	3
2	2	6	3	0	e	5	4	1
3	3	4	6	5	2	e	1	0
4	4	3	2	1	6	0	e	5
5	5	2	0	6	4	1	3	e
6	6	e	5	**4**	1	3	0	2

$0 \circ 3 = 5; 1 \circ 4 = 6; 6 \circ 2 = 4$

$0 \circ 0 = 1 \Rightarrow 4 \circ 6 = 5 \Rightarrow 3 \circ 3 = 2$
$0 \circ 2 = 3 \Rightarrow 6 \circ 1 = 5 \Rightarrow 5 \circ 3 = 4$
$0 \circ 4 = 2 \Rightarrow 1 \circ 0 = 5 \Rightarrow 4 \circ 3 = 6$
$0 \circ 5 = 6 \Rightarrow 2 \circ 4 = 5 \Rightarrow 1 \circ 3 = 0$
$0 \circ 6 = 4 \Rightarrow 3 \circ 2 = 5 \Rightarrow 6 \circ 3 = 1$
$1 \circ 1 = 4 \Rightarrow 5 \circ 2 = 6 \Rightarrow 6 \circ 4 = 3$
$1 \circ 5 = 2 \Rightarrow 2 \circ 0 = 6 \Rightarrow 4 \circ 4 = 0$
$1 \circ 6 = 3 \Rightarrow 3 \circ 1 = 6 \Rightarrow 5 \circ 4 = 1$
$2 \circ 1 = 3 \Rightarrow 5 \circ 1 = 0 \Rightarrow 5 \circ 5 = 3$
$2 \circ 2 = 0 \Rightarrow 6 \circ 5 = 0 \Rightarrow 2 \circ 5 = 4$
$2 \circ 6 = 1 \Rightarrow 3 \circ 6 = 0 \Rightarrow 3 \circ 5 = 1$
$3 \circ 0 = 4 \Rightarrow 4 \circ 2 = 1 \Rightarrow 6 \circ 6 = 2$
$4 \circ 0 = 3 \Rightarrow 4 \circ 1 = 2 \Rightarrow 5 \circ 0 = 2$

Fig. 2d.2.

Since there are $42 = 49-7$ cells to be filled with entries from the set $\{0, 1, 2, \ldots, 6\}$ and this is a multiple of three, either 0, 3, or 6 of the cells $(a, a+3)$ must have an entry of the form $a+5$. In our first example (which was originally given in [3] without any explanation as to how it was obtained), just three of the cells $(a, a+3)$ have $a+5$ as entry (see Figure 2d.2). In the example of Figure 2d.3, none of the cells $(a, a+3)$ have $a+5$ as entry.

$(\circ)$	e	0	1	2	3	4	5	6
e	e	0	1	2	3	4	5	6
0	0	1	e	4	6	5	2	3
1	1	6	3	e	5	2	0	4
2	2	5	4	3	e	0	6	1
3	3	4	5	6	2	e	1	0
4	4	3	2	1	0	6	e	5
5	5	2	6	0	1	3	4	e
6	6	e	0	5	4	1	3	2

$3 \circ 0 = 4 \Rightarrow 4 \circ 2 = 1 \Rightarrow 6 \circ 6 = 2$
$4 \circ 0 = 3 \Rightarrow 4 \circ 1 = 2 \Rightarrow 5 \circ 0 = 2$

$0 \circ 0 = 1 \Rightarrow 4 \circ 6 = 5 \Rightarrow 3 \circ 3 = 2$
$0 \circ 2 = 4 \Rightarrow 6 \circ 2 = 5 \Rightarrow 6 \circ 3 = 4$
$0 \circ 3 = 6 \Rightarrow 0 \circ 4 = 5 \Rightarrow 1 \circ 3 = 5$
$0 \circ 5 = 2 \Rightarrow 2 \circ 0 = 5 \Rightarrow 4 \circ 3 = 0$
$0 \circ 6 = 3 \Rightarrow 3 \circ 1 = 5 \Rightarrow 5 \circ 3 = 1$
$1 \circ 0 = 6 \Rightarrow 4 \circ 4 = 6 \Rightarrow 1 \circ 4 = 2$
$1 \circ 1 = 3 \Rightarrow 5 \circ 1 = 6 \Rightarrow 5 \circ 4 = 3$
$1 \circ 5 = 0 \Rightarrow 2 \circ 5 = 6 \Rightarrow 2 \circ 4 = 0$
$1 \circ 6 = 4 \Rightarrow 3 \circ 2 = 6 \Rightarrow 6 \circ 4 = 1$
$2 \circ 1 = 4 \Rightarrow 5 \circ 2 = 0 \Rightarrow 6 \circ 5 = 3$
$2 \circ 2 = 3 \Rightarrow 6 \circ 1 = 0 \Rightarrow 5 \circ 5 = 4$
$2 \circ 6 = 1 \Rightarrow 3 \circ 6 = 0 \Rightarrow 3 \circ 5 = 1$

Fig. 2d.3.

(e) m-inverse loops of order 9 with an inverse cycle of length 8.

We assume that $J = (e)(0\ 1\ 2\ \cdots\ 7)$ and that $0 \circ 2 = v$, $v \neq 0, 2$ or e as usual. Arithmetic is modulo 8.

When $n-1 = 8$ is relatively prime to $3m+1$: that is, when m is even, $0 \circ (v-1) = 7$ and $0 \circ (9-v) = 2-v$ by Lemma 2.1. Also, J is then an automorphism of the loop.

Neither $v = 1$ nor $v = 3$ is possible by Corollary 2.2. If $v = 4$, $0 \circ 2 = 4$, $0 \circ 3 = 7$ and $0 \circ 5 = 6$. If $v = 5$, $0 \circ 2 = 5$, $0 \circ 4 = 7$ and $0 \circ 4 = 5$; a contradiction. If $v = 6$, $0 \circ 2 = 6$, $0 \circ 5 = 7$ and $0 \circ 3 = 4$. If $v = 7$, $0 \circ 2 = 7$, $0 \circ 6 = 7$ and $0 \circ 2 = 3$; which are contradictory. Thus, when m is even, $v = 4$ or 6 are the only possibilities.

Since in general, by Lemma 2.1, the entry k in cell $(0, h)$ determines the entries in two other cells of row 0 and since there are all together seven cells of this row to be filled (see Figure 2e.1), one cell $(0, h)$ must have an entry k such that it coincides with the cells $(0, k-h+1)$ and $(0, n-k)$. Such a coincidence occurs only when $h = 6$ and $k = 3$. Thus, if $0 \circ 2 = 4$, $0 \circ 3 = 7$ and $0 \circ 5 = 6$ or if $0 \circ 2 = 6$, $0 \circ 5 = 7$ and $0 \circ 3 = 4$, we must also have $0 \circ 6 = 3$. To complete the entries of row 0, we require $0 \circ 0 = w$ where w is such that the elements $w+1$ and $9-w$ are 4 and 7 since the two remaining cells to be filled are $(0, 4)$ and $(0, 7)$. No such element w exists. We conclude that no 2, 4 or 6-inverse loops of order 9 with a long inverse cycle exist.

	e	0	1	2	3	4	5	6	7
e	e	0	1	2	3	4	5	6	7
0	0	·	e	·	·	·	·	·	·

Fig. 2e.1.

We look next at 1-inverse loops. For $a, b, c \neq e$, $a \circ b = c \Rightarrow (b-2) \circ (c-1) = (a-1) \Rightarrow (c-3) \circ (a-2) = (b-3) \Rightarrow (a-4) \circ (b-4) = (c-4)$ or $(a+4) \circ (b+4) = (c+4)$ since addition is modulo 4. That is, J^4 is an automorphism. Since J^8 is the identity, the multiplication of such a loop takes the form shown in Figure 2e.2.

	e	0	1	2	3	4	5	6	7
e	e	0	1	2	3	4	5	6	7
0	0								
1	1			A				B	
2	2								
3	3								
4	4								
5	5			$B+4$				$A+4$	
6	6								
7	7								

Fig. 2e.2.

However, we need to analyse the structure more precisely. In general, the entry in the cell (a, b) determines five other entries as follows:

$$a \circ b = c \qquad (b-2) \circ (c-1) = a-1 \qquad (c-3) \circ (a-2) = b-3$$
$$(a-4) \circ (b-4) = c-4 \qquad (b+2) \circ (c+3) = a+3 \qquad (c+1) \circ (a+2) = b+1$$

But $a \circ (a-2) = c \Rightarrow (a-4) \circ (c-1) = (a-1) \Rightarrow (c-3) \circ (a-2) = (a-5)$ so, if $c = a+3$, only two of the above six equalities are distinct. We have

$$a \circ (a-2) = a+3 \Rightarrow (a-4) \circ (a+2) = (a-1) \Rightarrow a \circ (a-2) = a-5 (\equiv a+3 \mod 8).$$

In the Cayley table of the loop, there are $64 - 8 = 56$ cells to be filled which do not contain the identity element e. Since $56 - 2$ or $56 - 8$ are divisible by 6, either two or all eight of the cells of type $(a, a-2)$ must have entry $a+3$.

We note further that $a \circ (a+2) = c \Rightarrow a \circ (c-1) = a-1$ so $c = a+3$ and $c = a-1$ respectively contradict the unique solubility for x of the equations $a \circ (a+2) = x$ and $a \circ x = a-1$. Thus, a cell of type $(a, a+2)$ must not contain either of the entries $a+3$ or $a-1$.

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

Fig. 2e.3.

Taking the above facts into consideration, our attempts to fill in the Cayley table by intelligent trial and error failed to yield a complete table but we were able to obtain two "almost" solutions. (One of these is shown in Figure 2e.3.) There appears to be no *a priori* reason why such loops should not exist despite the severe constraints just described.

It remains to resolve the much harder question of whether proper 3, 5 or 7-inverse loops of order 9 with a long inverse cycle exist.

(f) m-inverse loops of order 10 with an inverse cycle of length 9.

No such loops exist by Theorem 2.3.

(g) Summary of results regarding proper m-inverse loops, $m > 0$.

For all orders up to ten inclusive, proper m-inverse loops with a maximum length inverse cycle do not exist when $3m + 1$ is relatively prime to $n - 1$.

m-inverse loops of order $n = 3l + 1$ with a maximum length inverse cycle do not exist. (In particular, such loops do not exist of orders 7 and 10.)

For order 5, only 1-inverse loops exist. There are four isomorphically distinct such loops.

For order 6, only 3-inverse loops exist.

For order 8, only 2-inverse loops exist.

For order 9, 1-inverse loops may exist. The existence of proper 3, 5 or 7-inverse loops has not been investigated.

Our next theorem suggests that m-inverse loops with a maximum length inverse cycle probably do not exist when $3m + 1$ is relatively prime to $n - 1$ except possibly when n is very large.

Theorem 2.4 *An m-inverse loop of order n with $(0\,1\,2\cdots n-2)$ as long inverse cycle and with $J = (e)(0\,1\,2\cdots n-2)$ an automorphism can exist only if a cyclic neofield of the same order n exists.*

Proof. We may write the Cayley table of the m-inverse loop in the form shown in Figure 2g.1, where $f \circ g = a_{fg}$ for $f, g \in \{0, 1, \ldots, n-2\}$. Then, because J is an automorphism of the loop, $a_{i+1,j+1} = a_{ij} + 1$, where arithmetic of indices is modulo $n - 1$.

Let	Then
$p_1 = a_{03} - a_{02}$.	$p'_1 = p_1 - 1 = a_{03} - (a_{02} + 1) = a_{03} - a_{13} = a_{n-4,0} - a_{n-3,0}$.
$p_2 = a_{04} - a_{03}$.	$p'_2 = p_2 - 1 = a_{04} - (a_{03} + 1) = a_{04} - a_{14} = a_{n-5,0} - a_{n-4,0}$.
$p_3 = a_{05} - a_{04}$.	$p'_3 = p_3 - 1 = a_{05} - (a_{04} + 1) = a_{05} - a_{15} = a_{n-6,0} - a_{n-5,0}$.
$\ldots \quad \ldots \quad \ldots$	$\ldots \quad \ldots \quad \ldots \quad \ldots$
$p_{n-4} = a_{0,n-2} - a_{0,n-3}$.	$p'_{n-4} = p_{n-4} - 1 = a_{0,n-2} - (a_{0,n-3} + 1) = a_{10} - a_{20}$.
$p_{n-3} = a_{00} - a_{0,n-2}$.	$p'_{n-3} = p_{n-3} - 1 = a_{00} - (a_{0,n-2} + 1) = a_{00} - a_{10}$.

Since no two entries of the second row of the Cayley table are equal, no one of the p_i's is equal to zero. Since no two entries of the last column of the addition table are equal, no one of the p'_i's is equal to zero. Thus, for each i, $p_i \neq 0$ or 1;

so each $p_i \in \{2, 3, \ldots, n-2\}$. Also, the partial sums $p_1 = a_{03} - a_{02}, p_1 + p_2 = a_{04} - a_{02}, \ldots, p_1 + p_2 + \cdots + p_{n-4} = a_{0,n-2} - a_{02}$, $p_1 + p_2 + \cdots + p_{n-3} = a_{00} - a_{02}$ are all distinct and non-zero modulo n. Furthermore, the partial sums $p'_1 = a_{n-4,0} - a_{n-3,0}$, $p'_1 + p'_2 = a_{n-5,0} - a_{n-3,0}, \ldots, p'_1 + p'_2 + \cdots + p'_{n-3} = a_{00} - a_{n-3,0}$ are all distinct and non-zero modulo n.

	e	1	2	3	$\cdots$	$n-2$	0
e	e	1	2	3	$\cdots$	$n-2$	0
0	0	e	a_{02}	a_{03}	$\cdots$	$a_{0,n-2}$	a_{00}
1	1	a_{11}	e	a_{13}	$\cdots$	$a_{1,n-2}$	a_{10}
2	2	a_{21}	a_{22}	e	$\cdots$	$a_{2,n-2}$	a_{20}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$n-3$	$n-3$	$a_{n-3,1}$	$a_{n-3,2}$	$a_{n-3,3}$	$\cdots$	e	$a_{n-3,0}$
$n-2$	$n-2$	$a_{n-2,1}$	$a_{n-2,2}$	$a_{n-2,3}$	$\cdots$	$a_{n-2,n-2}$	e

Fig. 2g.1

We conclude that existence of an m-inverse loop of order n with $(0\,1\,2\cdots n-2)$ as long inverse cycle and with $J = (e)(0\,1\,2\cdots n-2)$ an automorphism implies that a subset of $n-3$ (not necessarily distinct) residues modulo $n-1$ from the set $\{2, 3, \ldots, n-2\}$ can be arranged in a sequence P such that:

(i) the partial sums of the first one, two, ... , $n-3$ elements are all distinct and non-zero modulo $n-1$; and

(ii) when each element of the sequence is reduced by one, the new sequence, P' say, also satisfies (i).

But these are exactly the conditions for existence of a cyclic neofield of order n. (See [2] or [5].) This proves the theorem.

Corollary. *An m-inverse loop of order n with $(0\,1\,2\cdots n-2)$ as long inverse cycle and with $J = (e)(0\,1\,2\cdots n-2)$ an automorphism exists if a cyclic neofield of the same order n exists whose addition table, $f \oplus g = a_{fg}$ for $f, g \neq e$, satisfies the further conditions that $a_{0h} = k$ implies that $a_{0,k-h+1} = n-h$ and $a_{0,n-h} = h-k$.*

Proof. The corollary follows directly from Theorem 2.4 and Lemma 2.1.

III. The existence of proper m-inverse quasigroups with a long inverse cycle, $m \geq 1$

We shall suppose that the elements of Q are $0, 1, \ldots, n-1$ and that the notation is chosen so that the long inverse cycle is $J = (0\,1\cdots n-1)$. Then $aJ = a+1 \mod n$ and $a \circ b = c \Rightarrow (a-m)J^m \circ [b-(m+1)]J^{m+1} = (c-m)J^m$.

But, $([b-(m+1)] \circ (c-m))J^m \circ [b-(m+1)]J^{m+1} = (c-m)J^m$ by the m-inverse

property. So, $[b-(m+1)]\circ(c-m)=a-m$. Iterating this result, we have

$$\begin{aligned} a\circ b=c &\Rightarrow [b-(m+1)]\circ(c-m)=a-m \\ &\Rightarrow [c-(2m+1)]\circ(a-2m)=b-(2m+1) \\ &\Rightarrow [a-(3m+1)]\circ[(b-(3m+1)]=[c-(3m+1)]. \end{aligned}$$

Thus, as was the case for loops, J^{3m+1} is an automorphism of any m-inverse quasigroup.

For an m-inverse quasigroup of order $3m+1$, the relation $[a-(3m+1)]\circ[(b-(3m+1)]=[c-(3m+1)]$ is equivalent to $a\circ b=c$ since, in such a quasigroup, arithmetic of elements is modulo $3m+1$.

For an m-inverse quasigroup of order n, where n is relatively prime to $3m+1$, the implication $a\circ b=c\Rightarrow[a-(3m+1)]\circ[(b-(3m+1)]=[c-(3m+1)]$ leads to the implication $a\circ b=c\Rightarrow(a+h)\circ(b+h)=(c+h)$ for all integers h by an argument exactly similar to the one we used for loops. Thus, in this case, J itself is an automorphism of the quasigroup. It also follows that such a quasigroup is $(m+l)$-inverse for all positive integers l.

Lemma 3.1 *In an m-inverse quasigroup (with a long inverse cycle) of order n, where n is relatively prime to $3m+1$, $0\circ h=k$ implies that $0\circ(k-h+1)=(n-h+1)$ and that $0\circ(n-k+1)=(n-k+h)$.*

Corollary 3.2 *When n is relatively prime to $3m+1$ in an m-inverse loop of order n with a long inverse cycle, $0\circ 2=3$ is impossible unless $n=4$.*

Proof. The proof of the Lemma is exactly similar to that of Lemma 2.1. It follows that $0\circ 2=3\Rightarrow 0\circ 2=n-1$ and $0\circ(n-2)=n-1$. These equations are contradictory except when $n=4$.

(a) m-inverse quasigroups of order 4 with an inverse cycle of length 4.

Here, $Q=\{0,1,2,3\}$ and $J=(0\,1\,2\,3)$. Arithmetic is modulo four. As for the case of loops, we shall suppose that $0\circ 2=v$.

We shall show that proper m-inverse quasigroups of order four with $m>1$ do not exist. However, there exist many proper 1-inverse quasigroups of order four. We may show this as follows:

We shall discuss only the case when $0\circ 2=1$. We observe that $0\circ 2=1\Rightarrow 0\circ 0=3\Rightarrow 2\circ 2=3$. These equalities require that $0\circ 1=0$ or 2 and that $1\circ 2=0$ or 2.

Case (a). $0\circ 1=2\Rightarrow 3\circ 1=3\Rightarrow 3\circ 2=2$, whence $1\circ 2\neq 2$ so $1\circ 2=0$ in this case. When $0\circ 1=2$ and $1\circ 2=0$, the multiplication table completes to a unique latin square as shown in Figure 3(a).1. Since $0\circ 3=0\Rightarrow 1\circ 3=3\Rightarrow 1\circ 2=0$, $1\circ 0=2\Rightarrow 2\circ 1=0\Rightarrow 3\circ 3=1$ and $1\circ 1=1\Rightarrow 3\circ 0=0\Rightarrow 2\circ 3=2$, the quasigroup so obtained is 1-inverse. Also, it is commutative.

It does not have the right inverse property, and so, as it is commutative, it is not 0-inverse. For example, $(0\circ 1)\circ 1J=(1\circ 0)\circ 1J=2\circ 2=3\neq 0$ and $(1\circ 0)\circ 0J=(0\circ 1)\circ 0J=2\circ 1=0\neq 1$. However, because it is commutative, it has a generalized right (and left) inverse property: namely, $(b\circ a)J\circ aJ^2=bJ$.

Case (b). $0 \circ 1 = 0$. Since $0 \circ 2 = 1$ and $0 \circ 0 = 3$, this forces $0 \circ 3 = 2$. Then we have

$$0 \circ 1 = 0 \Rightarrow 3 \circ 3 = 3 \Rightarrow 1 \circ 2 = 2 \quad \text{and} \quad 0 \circ 3 = 2 \Rightarrow 1 \circ 1 = 3 \Rightarrow 3 \circ 2 = 0,$$

as shown in Figure 3(a).2. This permits either $1 \circ 0 = 1$ or $1 \circ 0 = 0$.

In the former case, we have $1 \circ 0 = 1 \Rightarrow 2 \circ 0 = 0 \Rightarrow 2 \circ 3 = 1$, whence the entry in the cell $(2, 1)$ must be 2. Then $2 \circ 1 = 2 \Rightarrow 3 \circ 1 = 1 \Rightarrow 3 \circ 0 = 2$ in a 1-inverse quasigroup. The entry in the cell $(1, 3)$ is now forced to be 0. The Cayley table so obtained does represent a 1-inverse quasigroup since $1 \circ 3 = 0 \Rightarrow 1 \circ 3 = 0$ in such a quasigroup. This quasigroup is non-commutative. (See Figure 3(a).3.) It does not have the right inverse property and is not 0-inverse. For example, $(1 \circ 0) \circ 0J = 1 \circ 1 = 3 \neq 1$ and $(1 \circ 0) \circ 1J = 1 \circ 2 = 2 \neq 0$.

$(\circ)$	0	1	2	3
0	3	2	1	0
1	2^2	1^3	0	3^1
2	1^5	0^6	3	2^3
3	0^5	3	2	1^4

Fig. 3a.1.

$(\circ)$	0	1	2	3
0	3	0	1	2
1	·	3	2	·
2	·	·	3	·
3	·	·	0	3

Fig. 3a.2.

In the alternative case when $1 \circ 0 = 0$, we have $1 \circ 0 = 0 \Rightarrow 2 \circ 3 = 0 \Rightarrow 1 \circ 3 = 1$. There are two possible completions of the partial Cayley table so arising. (See Figure 3(a).4.) It is easy to check that both completions define proper 1-inverse quasigroups and that one is commutative and one not. (In fact, $2 \circ 0 = 1 \Rightarrow 2 \circ 0 = 1$, $2 \circ 1 = 2 \Rightarrow 3 \circ 1 = 1 \Rightarrow 3 \circ 0 = 2$ and, alternatively, $2 \circ 0 = 2 \Rightarrow 2 \circ 1 = 1 \Rightarrow 3 \circ 0 = 1$, $3 \circ 1 = 2 \Rightarrow 3 \circ 1 = 2$.)

$(\circ)$	0	1	2	3
0	3	0	1	2
1	1	3	2	0
2	0	2	3	1
3	2	1	0	3

Fig. 3a.3.

$(\circ)$	0	1	2	3
0	3	0	1	2
1	0	3	2	1
2	·	·	3	0
3	·	·	0	3

Fig. 3a.4.

As regards the existence of 2-inverse or 3-inverse quasigroups, we have $0 \circ 0 = u \Rightarrow 1 \circ (u-2) = 2 \Rightarrow (u-1) \circ 0 = 3$ for a 2-inverse quasigroup. If $u = 1$, $0 \circ 0 = 1 \Rightarrow 0 \circ 0 = 3$. If $u = 2, 0 \circ 0 = 2 \Rightarrow 1 \circ 0 = 2$. If $u = 3$, $0 \circ 0 = 3 \Rightarrow 2 \circ 0 = 3$. Each of these implications is contradictory. If $u = 0$, $0 \circ 0 = 0 \Rightarrow 1 \circ 2 = 2 \Rightarrow 3 \circ 0 = 3 \Rightarrow 1 \circ 1 = 1$. Because $3 \cdot 2 + 1 = 7$ is relatively prime to 4, J is an automorphism of the quasigroup and so we also have $2 \circ 2 = 2$ which contradicts $1 \circ 2 = 2$.

For a 3-inverse loop, $0 \circ 0 = u \Rightarrow -4 \circ (u-3) = -3 \Rightarrow (u-7) \circ (-2) = -3$. That is, $0 \circ 0 = u \Rightarrow 0 \circ (u+1) = 1 \Rightarrow (u+1) \circ 2 = 1$. J^{10} is an automorphism of such a quasigroup. Since J^4 is the identity mapping, it follows that J^2 is an automorphism.

If $u = 1$, $0 \circ 0 = 1 \Rightarrow 0 \circ 2 = 1$. If $u = 3$, $0 \circ 0 = 3 \Rightarrow 0 \circ 0 = 1$. Each of these is contradictory.

If $u = 2$, $0 \circ 0 = 2 \Rightarrow 0 \circ 3 = 1 \Rightarrow 3 \circ 2 = 1$. Using the fact that J^2 is an automorphism and that the body of the Cayley table must be a latin square, we find that we obtain the Cayley table given in Figure 3a.5. Similarly, if $u = 0$, $0 \circ 0 = 0 \Rightarrow 0 \circ 1 = 1 \Rightarrow 1 \circ 2 = 1$, we find that we obtain the Cayley table given in Figure 3a.6. Both Cayley tables represent 3-inverse quasigroups but neither is proper. Each is also 1-inverse. Thus, proper m-inverse quasigroups of order four with $m > 1$ do not exist, as we claimed.

$(\circ)$	0	1	2	3
0	2	0	3	1
1	3	1	2	0
2	1	3	0	2
3	0	2	1	3

Fig. 3a.5.

$(\circ)$	0	1	2	3
0	0	1	3	2
1	2	3	1	0
2	1	0	2	3
3	3	2	0	1

Fig. 3a.6.

(b) m-inverse quasigroups of order 5 with an inverse cycle of length 5.

We assume that $J = (0\,1\,2 \cdots 4)$ and that $0 \circ 2 = v$ as usual. Arithmetic is modulo 5.

When $n = 5$ is relatively prime to $3m+1$: that is, when $m \neq 5h+3$, $0 \circ (v-1) = 4$ and $0 \circ (6-v) = 2-v$ by Lemma 3.1. Also, J is an automorphism of the quasigroup.

If $v = 3$ or 4, the equalities $0 \circ 2 = v$ and $0 \circ (v-1) = 4$ contradict each other. When $v = 1$, the equalities $0 \circ 2 = v$ and $0 \circ (6-v) = 2-v$ contradict each other. When $v = 0$, $0 \circ 2 = 0$, $0 \circ 4 = 4$ and $0 \circ 1 = 2$ so the Cayley table takes the form shown in Figure 3b.1 which clearly cannot be completed. When $v = 2$, $0 \circ 2 = 2$, $0 \circ 1 = 4$ and $0 \circ 4 = 0$. In this case also, the Cayley table cannot be completed (see Figure 3b.2). Thus, no 1, 2 or 4-inverse quasigroups of order 5 with a long inverse cycle exist.

$(\circ)$	0	1	2	3	4
0	·	2	0	·	4
1	0	·	3	1	·
2	·	1	·	4	2
3	3	·	2	·	0
4	1	4	·	3	·

Fig. 3b.1.

$(\circ)$	0	1	2	3	4
0	·	4	2	·	0
1	1	·	0	3	·
2	·	2	·	1	4
3	0	·	3	·	2
4	3	1	·	4	·

Fig. 3b.2.

For a 3-inverse loop, the automorphism J^{10} is the identity because J^5 is the identity. We have $a \circ b = c \Rightarrow (b-4) \circ (c-3) = (a-3) \Rightarrow (c-2) \circ (a-1) = (b-2) \Rightarrow a \circ b = c$ so, in general, an entry c in cell (a, b) determines the entries in two other cells. However, $a \circ (a-1) = (a+2) \Rightarrow a \circ (a-1) = (a-3)$. Since $a + 2 \equiv a - 3 \mod 5$, an entry $a+2$ in cell $(a, a-1)$ determines no others. All together, there are

$25 = (8 \times 3) + 1 = (7 \times 3) + 4$ cells to be filled so either one or four of the cells of type $(a, a-1)$ must contain $a+2$. An example of a 3-inverse loop for which $0 \circ 2 = 1$ and four of the cells $(a, a-1)$ contain $a+2$ is given in Figure 3b.3.

$(\circ)$	0	1	2	3	4
0	3	0	1	4	**2**
1	2	1	4	0	3
2	0	**4**	2	3	1
3	1	3	**0**	2	4
4	4	2	3	**1**	0

$0 \circ 2 = 1 \Rightarrow 3 \circ 3 = 2 \Rightarrow 4 \circ 4 = 0$
$0 \circ 0 = 3 \Rightarrow 1 \circ 0 = 2 \Rightarrow 1 \circ 4 = 3$
$0 \circ 3 = 4 \Rightarrow 4 \circ 1 = 2 \Rightarrow 2 \circ 4 = 1$
$1 \circ 3 = 0 \Rightarrow 4 \circ 2 = 3 \Rightarrow 3 \circ 0 = 1$
$2 \circ 0 = 0 \Rightarrow 1 \circ 2 = 4 \Rightarrow 3 \circ 1 = 3$
$1 \circ 1 = 1 \Rightarrow 2 \circ 3 = 3 \Rightarrow 4 \circ 0 = 4$
$0 \circ 1 = 0 \Rightarrow 2 \circ 2 = 2 \Rightarrow 3 \circ 4 = 4$
$0 \circ 4 = 2; 2 \circ 1 = 4; 3 \circ 2 = 0; 4 \circ 3 = 1.$

Fig. 3b.3.

(c) m-inverse quasigroups of order 6 with an inverse cycle of length 6.

We assume that $J = (0\,1\,2 \cdots 5)$ and that $0 \circ 2 = v$ as usual. Arithmetic is modulo 6.

In this case, $n = 6$ is relatively prime to $3m+1$ for all values of m, so $0 \circ (v-1) = 5$ and $0 \circ (7-v) = 2-v$ by Lemma 3.1. Also, J is an automorphism of the quasigroup.

We find that when $v = 3$ or 5, the equalities $0 \circ 2 = v$ and $0 \circ (v-1) = 5$ contradict each other. When $v = 1$, the equalities $0 \circ 2 = v$ and $0 \circ (7-v) = 2-v$ contradict each other and, when $v = 4$, the equalities $0 \circ (v-1) = 5$ and $0 \circ (7-v) = 2-v$ contradict each other. When $v = 0$, $0 \circ 2 = 0$, $0 \circ 5 = 5$ and $0 \circ 1 = 2$. When $v = 2$, $0 \circ 2 = 2$, $0 \circ 1 = 5$ and $0 \circ 5 = 0$. Thus, $v = 0$ or 2 are the only possibilities.

Let $0 \circ 3 = w$. Then $0 \circ (w-2) = 4$ and $0 \circ (7-w) = 3-w$ by Lemma 3.1. When $v = 0$ or 2, we must have $w = 1$, 3 or 4. Each choice of w leads to a contradiction. For example, $0 \circ 3 = 1 \Rightarrow 0 \circ 5 = 4$ which is contradictory. Therefore, no m-inverse quasigroups of order 6 with an inverse cycle of length 6 exist.

(d) m-inverse quasigroups of order 7 with an inverse cycle of length 7.

We assume that $J = (0\,1\,2 \cdots 6)$ and that $0 \circ 2 = v$. Arithmetic is modulo 7.

When $n = 7$ is relatively prime to $3m+1$, $0 \circ (v-1) = 6$ and $0 \circ (8-v) = 2-v$ by Lemma 3.1. Also, J is an automorphism of the quasigroup. Since $0 \circ (v-1) = 6$, $v \neq 3$ or 6 otherwise $0 \circ 2 = v$ and $0 \circ (v-1) = 6$ are mutually contradictory. If $v = 1$, the equalities $0 \circ 2 = v$ and $0 \circ (8-v) = 2-v$ are mutually contradictory. Thus, $v \neq 1, 3, 6$.

If $v = 0$, $0 \circ 2 = 0$, $0 \circ 6 = 6$ and $0 \circ 1 = 2$. Because J is an automorphism of the quasigroup, $a \circ b = c \Rightarrow (a+h) \circ (b+h) = (c+h)$ and so the entries of the left-to-right broken diagonals headed by $0 \circ 2 = 0$, $0 \circ 6 = 6$ and $0 \circ 1 = 2$ in the Cayley table of the quasigroup are all determined. We find that the entries of the cells $(a, a+3)$ are then forced. In particular, $0 \circ 3 = 5$. By Lemma 3.1, $0 \circ 3 = 5$ does not determine any other entries of row 0. So $0 \circ 4 = 1$ or 3. By Lemma 3.1, $0 \circ 4 = 1$ implies that $0 \circ 5 = 4$ and $0 \circ 0 = 3$. We obtain the quasigroup illustrated in Figure 3d.1 which is a 0-inverse quasigroup (crossed-inverse quasigroup). Similarly,

$0 \circ 4 = 3$ implies that $0 \circ 0 = 4$ and $0 \circ 5 = 1$. We obtain the quasigroup illustrated in Figure 3d.2. This also is a 0-inverse quasigroup.

If $v = 2$, $0 \circ 2 = 2$, $0 \circ 1 = 6$ and $0 \circ 6 = 0$. Again the entries of the cells $(a, a+3)$ are forced and, in particular, $0 \circ 3 = 5$. Again $0 \circ 4 = 1$ or 3. We obtain two further 0-inverse quasigroups.

If $v = 4$, $0 \circ 2 = 4$, $0 \circ 3 = 6$ and $0 \circ 4 = 5$. Since J is an automorphism, these equalities respectively imply that $5 \circ 0 = 2$, $4 \circ 0 = 3$ and $3 \circ 0 = 1$. Also, they imply that $4 \circ 6 = 1$, $3 \circ 6 = 2$ and $2 \circ 6 = 0$. The equalities $0 \circ 0 = 0$ and $0 \circ 6 = 3$ are then forced. By Lemma 3.1, $0 \circ 0 = 0 \Rightarrow 0 \circ 1 = 1$ and $0 \circ 6 = 3 \Rightarrow 0 \circ 5 = 2$. The Cayley table cannot be completed since $0 \circ 0 = 0 \Rightarrow 1 \circ 1 = 1$ and $0 \circ 5 = 2 \Rightarrow 1 \circ 6 = 3$ because J is an automorphism.

If $v = 5$, we have $0 \circ 2 = 5$, $0 \circ 4 = 6$ and $0 \circ 3 = 4$ whence $5 \circ 0 = 3$, $3 \circ 0 = 2$ and $4 \circ 0 = 1$. Also, $4 \circ 6 = 2$, $2 \circ 6 = 1$ and $3 \circ 6 = 0$. $0 \circ 0 = 0$ and $0 \circ 6 = 3$ are again forced and the Cayley table cannot be completed.

$(\circ)$	0	1	2	3	4	5	6
0	3	2	0	5	1	4	6
1	0	4	3	1	6	2	5
2	6	1	5	4	2	0	3
3	4	0	2	6	5	3	1
4	2	5	1	3	0	6	4
5	5	3	6	2	4	1	0
6	1	6	4	0	3	5	2

Fig. 3d.1.

$(\circ)$	0	1	2	3	4	5	6
0	4	2	0	5	3	1	6
1	0	5	3	1	6	4	2
2	3	1	6	4	2	0	5
3	6	4	2	0	5	3	1
4	2	0	5	3	1	6	4
5	5	3	1	6	4	2	0
6	1	6	4	2	0	5	3

Fig. 3d.2.

Thus, no proper m-inverse quasigroups ($m > 0$) of order 7 with an inverse cycle of length 7 exist when $3m + 1$ is relatively prime to 7. This leaves the case when $m = 2$. In this case,

$$a \circ b = c \Rightarrow (b-3) \circ (c-2) = (a-2) \Rightarrow (c-5) \circ (a-4) = (b-5) \Rightarrow (a-7) \circ (b-7) = (c-7)$$

which is equivalent to $a \circ b = c$ since addition is modulo 7. Thus, in general, each relation $a \circ b = c$ implies two others. Therefore, putting entry c in cell (a, b) forces two other entries. However, $a \circ (a+3) = a+5 \Rightarrow a \circ (a+3) = a-2$. Since $a - 2 \equiv a + 5 \mod 7$, it is permissible to put the entry $a + 5$ in the cell $(a, a+3)$ without contradiction but such an entry forces no others.

$(\circ)$	0	1	2	3	4	5	6
0	1	3	0	**5**	2	6	4
1	5	4	2	0	**6**	3	1
2	2	6	1	4	5	**0**	3
3	3	0	5	2	1	4	6
4	0	1	3	6	4	2	5
5	4	5	6	3	0	1	2
6	6	2	**4**	1	3	5	0

$3 \circ 0 = 3 \Rightarrow 4 \circ 1 = 1 \Rightarrow 5 \circ 6 = 2$
$4 \circ 2 = 3 \Rightarrow 6 \circ 1 = 2 \Rightarrow 5 \circ 0 = 4$

$0 \circ 3 = 5; 1 \circ 4 = 6; 2 \circ 5 = 0; 6 \circ 2 = 4$

$0 \circ 0 = 1 \Rightarrow 4 \circ 6 = 5 \Rightarrow 3 \circ 3 = 2$
$0 \circ 1 = 3 \Rightarrow 5 \circ 1 = 5 \Rightarrow 5 \circ 3 = 3$
$0 \circ 2 = 0 \Rightarrow 6 \circ 5 = 5 \Rightarrow 2 \circ 3 = 4$
$0 \circ 4 = 2 \Rightarrow 1 \circ 0 = 5 \Rightarrow 4 \circ 3 = 6$
$0 \circ 5 = 6 \Rightarrow 2 \circ 4 = 5 \Rightarrow 1 \circ 3 = 0$
$0 \circ 6 = 4 \Rightarrow 3 \circ 2 = 5 \Rightarrow 6 \circ 3 = 1$
$1 \circ 1 = 4 \Rightarrow 5 \circ 2 = 6 \Rightarrow 6 \circ 4 = 3$
$1 \circ 2 = 2 \Rightarrow 6 \circ 0 = 6 \Rightarrow 4 \circ 4 = 4$
$1 \circ 5 = 3 \Rightarrow 2 \circ 1 = 6 \Rightarrow 5 \circ 4 = 0$
$1 \circ 6 = 1 \Rightarrow 3 \circ 6 = 6 \Rightarrow 3 \circ 4 = 1$
$2 \circ 0 = 2 \Rightarrow 4 \circ 0 = 0 \Rightarrow 4 \circ 5 = 2$
$2 \circ 2 = 1 \Rightarrow 6 \circ 6 = 0 \Rightarrow 3 \circ 5 = 4$
$2 \circ 6 = 3 \Rightarrow 3 \circ 1 = 0 \Rightarrow 5 \circ 5 = 1$

Fig. 3d.3.

Since there are $49 = 48 + 1 = 45 + 4 = 42 + 7$ cells to be filled with entries from the set $\{0, 1, 2, \ldots, 6\}$ and this is not a multiple of three, either 1, 4, or 7 of the cells $(a, a+3)$ must have an entry of the form $a+5$. In our example above (Figure 3d.3), just four of the cells $(a, a+3)$ have $a+5$ as entry.

It is easy to check that the above quasigroup is not 0-inverse. For example, $(0 \circ 1) \circ 0J = 3 \circ 1 = 0 \neq 1$.

(e) m-inverse quasigroups of order 8 with an inverse cycle of length 8.

We assume that $J = (0\,1\,2 \cdots 7)$ and that $0 \circ 2 = v$. Arithmetic is modulo 8.

When $n = 8$ is relatively prime to $3m+1$: that is, when m is even, $0 \circ (v-1) = 7$ and $0 \circ (9 - v) = 2 - v$ by Lemma 3.1. Also, J is then an automorphism of the quasigroup.

If $v = 0$, $0 \circ 2 = 0$, $0 \circ 7 = 7$ and $0 \circ 1 = 2$. If $v = 1$, $0 \circ 2 = 1$, $0 \circ 0 = 7$ and $0 \circ 0 = 1$; which are contradictory. If $v = 2$, $0 \circ 2 = 2$, $0 \circ 1 = 7$ and $0 \circ 7 = 0$. If $v = 3$, $0 \circ 2 = 3$, $0 \circ 2 = 7$ and $0 \circ 6 = 7$; which are contradictory (as in Corollary 3.2). If $v = 4$, $0 \circ 2 = 4$, $0 \circ 3 = 7$ and $0 \circ 5 = 6$. If $v = 5$, $0 \circ 2 = 5$, $0 \circ 4 = 7$ and $0 \circ 4 = 5$; a contradiction. If $v = 6$, $0 \circ 2 = 6$, $0 \circ 5 = 7$ and $0 \circ 3 = 4$. If $v = 7$, $0 \circ 2 = 7$, $0 \circ 6 = 7$ and $0 \circ 2 = 3$; which are contradictory. Thus, when m is even, $v = 0, 2, 4$ or 6 are the only possibilities.

Since in general, by Lemma 3.1, the entry k in cell $(0, h)$ determines the entries $9-h$ and $8-k+h$ in the two other cells $(0, k-h+1)$ and $(0, 9-k)$ of row 0 and since there are all together eight cells of this row to be filled, some coincidences among these cells must occur. However, such a coincidence occurs only when $h = 6$ and $k = 3$ and then all three of the cells coincide. In each of the possible cases $v = 0, 2, 4$ or 6, this leaves four cells of row 0 to be filled. Since each remaining cell that is filled determines two others distinct from it that are also filled, it is impossible to complete row 0 in such a way as to define a 2, 4 or 6-inverse quasigroup. We conclude that no 2, 4 or 6-inverse quasigroups of order 8 with a long inverse cycle exist.

	0	1	2	3	4	5	6	7
0								
1			A				B	
2								
3								
4								
5			$B+4$				$A+4$	
6								
7								

Fig. 3e.1.

We look next at 1-inverse quasigroups. We have $a \circ b = c \Rightarrow (b-2) \circ (c-1) = (a-1) \Rightarrow (c-3) \circ (a-2) = (b-3) \Rightarrow (a-4) \circ (b-4) = (c-4)$ or $(a+4) \circ (b+4) = (c+4)$ since addition is modulo 4. That is, J^4 is an automorphism. Since J^8 is the identity, the multiplication of such a quasigroup takes the form shown in Figure 3e.1. However, we need to analyse the structure more precisely (cf. 1-inverse loops of order 9). In general, the entry in the cell (a, b) determines five other entries as follows:

$$a \circ b = c \qquad (b-2) \circ (c-1) = a-1 \qquad (c-3) \circ (a-2) = b-3$$

$$(a-4) \circ (b-4) = c-4 \qquad (b+2) \circ (c+3) = a+3 \qquad (c+1) \circ (a+2) = b+1$$

Since $J = (0\,1\,2 \cdots 7)$, we have

$$a \circ (a-2) = a+3 \Rightarrow (a-4) \circ (a+2) = (a-1) \Rightarrow a \circ (a-2) = a-5 (\equiv a+3 \mod 8)$$

as in the case of loops of order 9. The entry c in each other cell (a, b), $b \neq a-2$, determines five others. There are 64 cells to be filled so, since $64-4 = 60$ is divisible by 6 and there are only eight cells of type $(a, a-2)$, just four of these latter must contain the entry $a+3$.

Also, as in the case of a 1-inverse loop of order 9, no cell of type $(a, a+2)$ can contain an entry $a+3$ or $a-1$ otherwise unique solubility of equations is contradicted.

Quasigroups satisfying these necessary conditions do exist. An example is given in Figure 3e.2.

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

Fig. 3e.2.

It remains to resolve the much harder question of whether proper 3, 5 or 7-inverse quasigroups of order 8 with a long inverse cycle exist (cf. loops of order 9 with a long inverse cycle).

(f) m-inverse quasigroups of order 9 with an inverse cycle of length 9.

We assume that $J = (0\,1\,2\,\cdots\,8)$. Arithmetic is modulo 9. Let $0\circ1 = u$, $0\circ2 = v$, $0 \circ 3 = w$ and $0 \circ 4 = x$. Since $n = 9$ is relatively prime to $3m + 1$ for all values of m, we can make use of Lemma 3.1 so

$$0 \circ 1 = u \Rightarrow 0 \circ u = 0 \Rightarrow 0 \circ (1 - u) = 1 - u \quad (\Rightarrow 0 \circ 1 = u);$$
$$0 \circ 2 = v \Rightarrow 0 \circ (v - 1) = 8 \Rightarrow 0 \circ (1 - v) = 2 - v \quad (\Rightarrow 0 \circ 2 = v);$$
$$0 \circ 3 = w \Rightarrow 0 \circ (w - 2) = 7 \Rightarrow 0 \circ (1 - w) = 3 - w \quad (\Rightarrow 0 \circ 3 = w);$$
$$0 \circ 4 = x \Rightarrow 0 \circ (x - 3) = 6 \Rightarrow 0 \circ (1 - x) = 4 - x \quad (\Rightarrow 0 \circ 4 = x).$$

Also, J is an automorphism of the quasigroup.

We find that $u = 0, 1, 5$; $v = 1, 3, 8$; $w = 5, 6, 7$; and $x = 2, 6, 7$ lead immediately to contradictions.

Case (a) $0 \circ 1 = 2 \Rightarrow 0 \circ 2 = 0$ and $0 \circ 8 = 8$.
Case (b) $0 \circ 1 = 3 \Rightarrow 0 \circ 3 = 0$ and $0 \circ 7 = 7$.
Case (c) $0 \circ 1 = 4 \Rightarrow 0 \circ 4 = 0$ and $0 \circ 6 = 6$.
Case (d) $0 \circ 1 = 6 \Rightarrow 0 \circ 6 = 0$ and $0 \circ 4 = 4$.
Case (e) $0 \circ 1 = 7 \Rightarrow 0 \circ 7 = 0$ and $0 \circ 3 = 3$.
Case (f) $0 \circ 1 = 8 \Rightarrow 0 \circ 8 = 0$ and $0 \circ 2 = 2$.

Case (A) $0 \circ 2 = 4 \Rightarrow 0 \circ 3 = 8$ and $0 \circ 6 = 7$.
Case (B) $0 \circ 2 = 5 \Rightarrow 0 \circ 4 = 8$ and $0 \circ 5 = 6$.
Case (C) $0 \circ 2 = 6 \Rightarrow 0 \circ 5 = 8$ and $0 \circ 4 = 5$.
Case (D) $0 \circ 2 = 7 \Rightarrow 0 \circ 6 = 8$ and $0 \circ 3 = 4$.
(The remaining values of $0 \circ 2$ are already covered or lead to contradictions.)

$0 \circ 3 = 1 \Rightarrow 0 \circ 8 = 7$ and $0 \circ 0 = 2$. $\quad$ $0 \circ 4 = 1 \Rightarrow 0 \circ 7 = 6$ and $0 \circ 0 = 3$.
$0 \circ 3 = 2 \Rightarrow 0 \circ 0 = 7$ and $0 \circ 8 = 1$. $\quad$ $0 \circ 4 = 3 \Rightarrow 0 \circ 0 = 6$ and $0 \circ 7 = 1$.
(The remaining values of $0 \circ 3$ and $0 \circ 4$ are already covered.)

Trial of the various cases shows that the first row of the Cayley table (that representing the products $0 \circ z$) cannot be completed. For example, if Case (a) is assumed, then the two possible entries for $0 \circ 3$ give contradictions. If Case (b) is assumed, then Cases (A) and (D) are not possible. If $0 \circ 2 = 5$ (Case (B)), then $0\circ1 = 3$, $0\circ2 = 5$, $0\circ3 = 0$, $0\circ4 = 8$, $0\circ5 = 6$ and $0\circ7 = 7$, so $0\circ0 = 1, 2$ or 4. By Lemma 3.1, $0 \circ 0 = 1 \Rightarrow 0 \circ 2 = 1$, $0 \circ 0 = 2 \Rightarrow 0 \circ 3 = 1$, $0 \circ 0 = 4 \Rightarrow 0 \circ 5 = 1$, all of which are contradictory. If $0 \circ 2 = 6$ (Case (C)), then $0 \circ 1 = 3$, $0 \circ 2 = 6$, $0 \circ 3 = 0$, $0 \circ 4 = 5$, $0 \circ 5 = 8$ and $0 \circ 7 = 7$, so $0 \circ 0 = 1, 2$ or 4 as before and each of these values leads to a contradiction.

We conclude that no m-inverse quasigroups of order 9 with an inverse cycle of length 9 exist.

(g) Summary of results regarding proper m-inverse quasigroups with a maximum length inverse cycle,$m > 0$.

For all orders up to nine inclusive, proper m-inverse quasigroups with a maximum length inverse cycle do not exist when $3m + 1$ is relatively prime to n.

For order 4, only 1-inverse quasigroups exist.

For order 5, only 3-inverse quasigroups exist.

For order 6, no m-inverse quasigroups ($m > 0$) exist.

For order 7, only 2-inverse quasigroups exist.

For order 8, 1-inverse quasigroups exist. There are no 2, 4 or 6-inverse quasigroups. The existence of proper 3, 5 or 7-inverse quasigroups remains to be investigated.

For order 9, no m-inverse quasigroups exist.

Note. Our investigation of the case when $n = 7$ shows that it is probable that, for larger n, proper m-inverse quasigroups ($m > 0$) with an inverse cycle of maximum length do exist when $3m + 1$ is relatively prime to n.

IV. A direct product construction

Let $(Q_1, \circ)$ and $(Q_2, \times)$ be m-inverse quasigroups with respect to the permutations J_1, J_2 of Q_1, Q_2 respectively. Define $(x_1, x_2)J = (x_1J_1, x_2J_2)$, where J is a permutation of $Q_1 \times Q_2$. Let $|Q_1| = n_1$ and $|Q_2| = n_2$.

We may define a binary operation $(\otimes)$ on $Q_1 \times Q_2$ by $(x_1, x_2) \otimes (y_1, y_2) = (x_1 \circ y_1, x_2 \times y_2)$. Then, since $(x_1 \circ y_1)J_1^m \circ x_1J_1^{m+1} = y_1J_1^m$ and $(x_2 \times y_2)J_2^m \times x_2J_2^{m+1} = y_2J_2^m$, we have

$$\begin{aligned}
[(x_1, x_2) \otimes (y_1, y_2)]J^m \otimes (x_1, x_2)J^{m+1} & \\
&= (x_1 \circ y_1, x_2 \times y_2)J^m \otimes (x_1, x_2)J^{m+1} \\
&= [(x_1 \circ y_1)J_1^m, (x_2 \times y_2)J_2^m] \otimes (x_1J_1^{m+1}, x_2J_2^{m+1}) \\
&= [(x_1 \circ y_1)J_1^m \circ x_1J_1^{m+1}, (x_2 \times y_2)J_2^m \times x_2J_2^{m+1}] \\
&= (y_1J_1^m, y_2J_2^m) \\
&= (y_1, y_2)J^m.
\end{aligned}$$

Thus, $(Q_1 \times Q_2, \otimes)$ is an m-inverse quasigroup of order n_1n_2 relative to the permutation J of $Q_1 \times Q_2$. Moreover, if at least one of $(Q_1, \circ)$ and $(Q_2, \times)$ is proper, then the direct product will be proper.

If J_1 defines a long inverse cycle of length h_1 of $(Q_1, \circ)$ and J_2 defines a long inverse cycle of length h_2 of $(Q_2, \times)$, then J defines an inverse cycle of $(Q_1 \times Q_2, \otimes)$ of length equal to the least common multiple of h_1 and h_2.

We have proved:

Theorem 4.1 *Let $(Q_1, \circ)$ and $(Q_2, \times)$ be m-inverse quasigroups with respect to the permutations J_1, J_2 of Q_1, Q_2 respectively of which at least one is proper. Then, their direct product will be a proper m-inverse quasigroup with respect to the permutation J of $Q_1 \times Q_2$ defined by $(x_1, x_2)J = (x_1J_1, x_2J_2)$.*

Example 4.1 Let $(Q_1, \circ)$ and $(Q_2, \times)$ be respectively the 0-inverse quasigroup of order 7 whose Cayley table is given in Figure 3d.1 and the proper 3-inverse quasigroup of order 5 whose Cayley table is given in Figure 3b.3. Since every 0-inverse quasigroup $(Q_1, \circ)$ is also a 3-inverse quasigroup (because the permutation J_1 is an automorphism), the direct product is a proper 3-inverse quaigroup of order 35 and has a long inverse cycle of length 35 (equal to the LCM of 7 and 5).

Clearly, we may use a similar procedure to obtain the direct product of any number of m-inverse quasigroups.

V. A generalization: (r, s, t)-quasigroups

We may generalize the concept of an m-inverse quasigroup in the following way:

Definition. Suppose that there exists a permutation J of the elements of a quasigroup $(Q, \circ)$ such that, for all $a, b \in Q$, $(a \circ b)J^r \circ aJ^s = bJ^t$. Then $(Q, \circ)$ is an (r, s, t)-*inverse quasigroup.*

Let us first observe that

Lemma 5.1 *An (r, s, t)-inverse loop $(L, \circ)$ with identity element e in which $a \circ aJ = e$ for all $a \in L$ is an r-inverse loop.*

Proof. Suppose that $(a \circ b)J^r \circ aJ^s = bJ^t$ (Equation 1) for all pairs of elements a, b in a loop with identity element e. Since $e \circ eJ = e$, we have $eJ = e$ and so $eJ^u = e$ for all positive integers u. If we put $a = e$ in Equation 1, we get $bJ^r \circ eJ^s = bJ^t$. That is, $bJ^r \circ e = bJ^t$. Therefore, $bJ^r = bJ^t$ and so $t = r$. If we put $b = e$ in Equation 1, we get $aJ^r \circ aJ^s = eJ^t = e$ and so $aJ^s = (aJ^r)J$. It follows that $s = r + 1$.

Thus, $s = r + 1$ and $t = r$ so the loop is r-inverse.

We shall discuss the construction of (r, s, t)-inverse quasigroups in a forthcoming paper.

References

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

[2] D. Bedford, Ph.D. Thesis, University of Surrey, 1991.

[3] B.B. Karklinüsh and V.B. Karklin, Inverse loops (in Russian). In "Nets and Quasigroups", Mat. Issl. 39(1976), 82–86.

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

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

(Received 23/5/2001)