PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 68, Number 2, February 1978

INVERSE-CYCLES IN WEAK-INVERSE LOOPS

R. ARTZY

ABSTRACT. In a loop let J be the map taking every element into its right inverse. If the order of J is n, then $\{x, xJ, \ldots, xJ^{n-1}\}$ is called an inverse-cycle of length n. If a weak-inverse loop consists only of the unit element and m inverse-cycles of length n, then n divides $2m$.

In a loop $(L, \cdot)$ with unit element e, let J be the bijection defined by $L \to L$, $x \mapsto xJ$, $x \cdot xJ = e$. If n is the least positive integer for which $xJ^n = x$, we call $\{xJ^r | r \in Z\}$ an *inverse-cycle* of length n. *Weak-inverse* (WI) loops, as introduced in [**1**], are defined by the identity $y \cdot (xy)J = xJ$. In this note a necessary condition will be established for a finite WI loop to consist only of e and inverse-cycles of equal lengths. In view of the many applications of WI loops and of the simple structure of the automorphism group if a WI loop consists only of such inverse-cycles, the result should be useful for dealing with finite loops.

First we note two well-known facts: (i) In every WI loop, J^2 is an automorphism [**1**]. (ii) Every cross-inverse (CI) loop, that is, a loop satisfying one of the equivalent identities $x(y \cdot xJ) = y$, $xy \cdot xJ = y$, is WI; however, there are WI loops (for instance, nonabelian groups) which are not CI.

LEMMA. *Let a WI loop consist only of e and inverse-cycles of length n. If n is odd, J is an automorphism, and the loop is CI.*

PROOF. Let $n = 2k + 1$. Then $J = J^{2k+1}(J^2)^{-k} = J^n(J^2)^{-k}$. Now $J^n = \mathrm{id}$ and J^2 is an automorphism, hence J itself is an automorphism. We have identically

$$xJ = y \cdot (xy)J = y(xJ \cdot yJ),$$

which is the first CI identity.

THEOREM. *A necessary condition for a WI loop that is not CI to consist only of e and m inverse-cycles of length n is $n|2m$.*

PROOF. First, we note that, in view of the Lemma, n is even. Let $x_1, \ldots, x_m$ be representatives of the m inverse-cycles. Define the functions f and g by

$$x_pJ^k \cdot x_q = x_rJ^{f(p,k,q)-1}, \tag{1}$$

$$x_pJ^{k+1} \cdot x_qJ = x_rJ^{g(p,k,q)}. \tag{2}$$

Received by the editors May 2, 1977.
AMS (MOS) subject classifications (1970). Primary 20N05.

(We disregard here those equations in which the right-hand side is e.) Then the WI identity and the fact of J^2 being an automorphism yield

$$x_q J^{-f(p,k,q)} \cdot x_r = x_p J^{k+1-f(p,k,q)} \quad \text{for even } f(p,k,q), \tag{3}$$

$$x_q J^{1-f(p,k,q)} \cdot x_r J = x_p J^{k+2-f(p,k,q)} \quad \text{for odd } f(p,k,q), \tag{4}$$

$$x_q J^{1-g(p,k,q)} \cdot x_r J = x_p J^{k+2-g(p,k,q)} \quad \text{for even } g(p,k,q), \tag{5}$$

$$x_q J^{-g(p,k,q)} \cdot x_r = x_p J^{k+1-g(p,k,q)} \quad \text{for odd } g(p,k,q). \tag{6}$$

Equations (3) through (6) have to be understood mod n. Using the definitions of f and g we obtain from (3) through (6), respectively, again mod n:

$$k + 2 - f(p,k,q) = f(q, -f(p,k,q), r),$$

$$k + 2 - f(p,k,q) = g(q, -f(p,k,q), r),$$

$$k + 2 - g(p,k,q) = g(q, -g(p,k,q), r),$$

$$k + 2 - g(p,k,q) = f(q, -g(p,k,q), r).$$

Let q be fixed. Then $f(p,k,q)$ and $g(p,k,q)$ run through all of $\{0, \ldots, n-1\}$, other than the value 1 in the case $q = r$, because then (1) and (2) become impossible. Summing for all p and k yields therefore

$$\sum_{p,k} f(p,k,q) = \sum_{p,k} g(p,k,q) = mn(n-1)/2 - 1. \tag{7}$$

Summing the left-hand sides of (3′) through (6′) for fixed q we get $\Sigma k + \Sigma 2 - \Sigma f(p,k,q) - \Sigma g(p,k,q)$. In (1) and (2), k ranges through all values mod n, other than $k = -1$ for $p = q$. For fixed q the number of equations (1) is therefore $mn - 1$, and so is the number of equations (2). Hence for fixed q we have

$$\sum k = mn(n-1)/2 - (-1) + mn(n-1)/2 - (-1) = 2 \pmod n$$

and $\Sigma 2 = 2(2mn - 2) = -4 \pmod n$. Thus the sum of the left-hand sides of (3′) through (6′) for fixed q is

$$2 - 4 - mn(n-1) + 2 = 0 \pmod n.$$

Summing the left-hand sides for all q, we obtain $m \cdot 0 = 0 \pmod n$.

In order to perform the summation of the right-hand sides of (3′) through (6′) we observe that $f(p,k,q)$ and $g(p,k,q)$ are defined for all values of p, k, and q except the cases where $p = q$ and simultaneously $k = -1$. Let Z_n be the additive cyclic group of order n, and $S := \{1, 2, \ldots, m\}$. Then we claim that the maps

$$(S \times Z_n \times S) \setminus \{(s, -1, s) | s \in S\} \to (S \times Z_n \times S) \setminus \{(s, -1, s) | s \in S\},$$

ϕ_1: $(p,k,q) \mapsto (q, -f(p,k,q), r)$ and ϕ_2: $(p,k,q) \mapsto (q, -g(p,k,q), r)$ are bijective. Indeed, (1) and (2), other than in the case $p = q$, $k = -1$, show that ϕ_1 and ϕ_2 are injective. Furthermore, given $q, f(p,k,q), r$, or $q, g(p,k,q), r$, respectively, equations (1) and (2) determine p, k, q uniquely unless $f(p,k,q)$ or $g(p,k,q)$, respectively, assume the value 1. This proves the surjectivity of ϕ_1 and ϕ_2. Thus the right-hand sides of (3′) through (6′) are $f(a, b, c)$ and $g(a, b, c)$ for all possible values of $(a, b, c) \in (S \times Z_n \times S) \setminus \{(s, -1, s) | s \in S\}$. The number of summands is $2(m^2n - m)$, and in view of (7), their sum is

$$m^2n(n-1) - 2m = -2m \pmod n.$$

Equating the sums of the two sides of all (3′) through (6′) yields, therefore, $0 = -2m \pmod n$, that is, $n|2m$.

COROLLARY. *The necessary condition mentioned in the Theorem holds for all WI loops.*

PROOF. This was proved for CI loops in [2]; the rest follows from the Theorem.

No example of a finite CI loop consisting of e and m inverse-cycles of equal length $n > 2$ is known. However, the following is an example of a WI loop, not CI, with $m = 2$, $n = 4$.

e	1 2 3 4	5 6 7 8
1	5 e 8 6	3 2 4 7
2	8 6 e 5	4 7 3 1
3	6 8 7 e	2 5 1 4
4	e 7 6 8	1 3 2 5
5	3 1 4 2	7 e 8 6
6	7 5 2 1	8 4 e 3
7	2 4 1 3	6 8 5 e
8	4 3 5 7	e 1 6 2

ADDED IN PROOF. Ehud Artzy (SUNY at Buffalo) has found examples of WI loops, CI and non-CI, with $m = n = 4$.

REFERENCES

1. J. M. Osborn, *Loops with the weak inverse property*, Pacific J. Math. **10** (1960), 295–304.
2. R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448–453.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAIFA, 31999 HAIFA, ISRAEL