Quasigroups and Related Systems **21** (2013), 97 − 102

Nuclei and commutants of C-loops

Muhammad Shah, Asif Ali and Volker Sorge

Abstract. C-loops are loops that satisfy the identity $x(y(yz)) = ((xy)y)z$. In this note we use the order of nuclei of C-loops to show that (1) nonassociative C-loops of order $2p$, where p is prime, are Steiner loops, (2) nonassociative C-loops of order $3n$ are non-simple and non-Steiner, (3) no nonassociative C-loop of order $2{\cdot}3^t$, $t \geqslant 1$ exists, and (4) if every element of the commutant of a C-loop is of odd order the commutant forms a subloop.

1. Introduction

C-*loops* are loops satisfying the identity $x(y(yz)) = ((xy)y)z$. The nature of the identity, where unlike in other Bol-Moufang identities the repeated variable is not separated by either of the other variables, makes them a difficult target of study. Nevertheless they have been investigated in [1, 2, 3, 4, 6, 9, 10, 12, 13, 14, 15].

In this note we extend some results of [14], in particular [14, Proposition 3.1] that states that only even order nonassociative C-loops exist. Investigating this result further using the order of nuclei of C-loops, we prove that (1) all nonassociative C-loops of order $2p$, where p is prime, are Steiner loops, (2) all nonassociative C-loops of order $3n$ are non-simple and non-Steiner, (3) there exists no nonassociative C-loop of order $2 \cdot 3^t$, $t \geqslant 1$, and (4) if $C(L)$ is the commutant of a C-loop L and every element of $C(L)$ is of odd order, then $C(L)$ is a subloop of L.

All examples presented in this paper have been computed by FINDER [16] and verified by GAP [11].

2. Preliminaries

In this paper we are concerned exclusively with finite loops. Let L be a loop we then define *left nucleus* N_λ, *middle nucleus* N_μ, and *right nucleus* N_ρ of L as the sets

$$N_\lambda = \{x \in L; x(yz) = (xy)z \text{ for every } y, z \in L\},$$
$$N_\mu = \{x \in L; y(xz) = (yx)z \text{ for every } y, z \in L\},$$
$$N_\rho = \{x \in L; y(zx) = (yz)x \text{ for every } y, z \in L\}.$$

2010 Mathematics Subject Classification: 20N99
Keywords: C-loop, nucleus, Steiner loop, commutant.

The *nucleus* N of L is the defined as $N = N_\lambda \cap N_\mu \cap N_\rho$. N is subgroup of L and, in particular, for C-loops we have $N = N_\lambda = N_\mu = N_\rho$.

We also define the *commutant* $C(L)$ of a loop L to be the set

$$C(L) = \{c \in L : cx = xc \text{ for every } x \in L\}.$$

The following hold for a C-loop L with commutant $C(L)$ and nucleus N.

(i) There is no C-loop with nucleus of index 2 [14, Lemma 2.9].

(ii) $C(L)$ is a normal subgroup of L [14, Proposition 2.7].

(iii) If L is nonassociative, of order n and N of order m. Then

- (a) $n/m \equiv 2(\text{mod } 6)$ or $n/m \equiv 4(\text{mod } 6)$,
- (b) n is even, and
- (c) if $n = pk$ for some prime p and positive integer k, then $p = 2$ and $k > 3$ [14, Proposition 3.1].

Moreover, there is a nonassociative non-Steiner C-loop of order $2k$ for every $k > 3$.

3. Nucleus of C-loops

We start our considerations with a corollary to [14, Proposition 3.1].

Corollary 3.1. *Let L be a nonassociative C-loop of order n with nucleus N of order m. Then*

(i) $n/m \equiv 1(\text{mod}3)$ *or* $n/m \equiv 2(\text{mod}3)$,

(ii) $(n/2)/m$ *is an integer of the form* $3k-1$ *or* $3k+1$,

(iii) $(n/m)^2 \equiv 4(\text{mod}6)$ *or* $n/m \equiv 4(\text{mod}6)$,

(iv) n/m *is of the form* $2(3k-1)$ *or* $(n/m)^2$ *is of the form* $2(3k-1)$.

Proof. (i) and (iii) are straightforward.
(ii) We have

$$\begin{aligned}
n/m &\equiv 2(\text{mod}6) \text{ or } n/m \equiv 4(\text{mod}6)\\
n/m &= 6k+2 \text{ or } n/m = 6k+4 \text{ for some positive integer } k\\
n/m &= 2(3k+1) \text{ or } n/m = 2(3k+2)\\
n/2m &= 3k+1 \text{ or } n/2m = 3k+2\\
(n/2)/m &= 3k+1 \text{ or } (n/2)/m = 3k+2. \text{ But every integer of the form}\\
&\quad 3k+2 \text{ is also of the form } 3k-1.
\end{aligned}$$

Thus $(n/2)/m = 3k+1$ or $(n/2)/m = 3k-1$.
(iv) By part (iii), we have

$$\begin{aligned}
(n/m)^2 &\equiv 4(\text{mod}6) \text{ or } n/m \equiv 4(\text{mod}6)\\
(n/m)^2 &= 6k+4 \text{ or } n/m = 6k+4 \text{ for some positive integer } k\\
(n/m)^2 &= 2(3k+2) \text{ or } n/m = 2(3k+2)\\
(n/m)^2 &= 2(3k-1) \text{ or } n/m = 2(3k-1).
\end{aligned}$$

□

Proposition 3.2. *A nonassociative C-loop L of order $3n$ is non-simple and non-Steiner.*

Proof. $L/N(L)$ is Steiner, hence $3n/m$ is congruent to 2 or 4 mod 6. So $3n/m$ is not divisible by 3, thus m is divisible by 3. Therefore, $N(L)$ is a group containing an element of order 3 and hence L is not Steiner. Since $N(L)$ is nontrivial and since $N(L)$ is normal in L by [14], it follows that L is not simple. □

The following example illustrates the above proposition.

Example 3.3. A nonassociative, noncommutative, non-Steiner non-simple C-loop of order 12 (size of nucleus = 3) is given in Table 1.

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	0	1	2	9	10	11	6	7	8
4	4	5	3	1	2	0	10	11	9	7	8	6
5	5	3	4	2	0	1	11	9	10	8	6	7
6	6	7	8	10	11	9	0	1	2	5	3	4
7	7	8	6	11	9	10	1	2	0	3	4	5
8	8	6	7	9	10	11	2	0	1	4	5	3
9	9	10	11	8	6	7	3	4	5	2	0	1
10	10	11	9	6	7	8	4	5	3	0	1	2
11	11	9	10	7	8	6	5	3	4	1	2	0

Table 1:

$\cdot$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	9	8	7	6
2	2	3	0	1	6	8	4	9	5	7
3	3	2	1	0	7	9	8	4	6	5
4	4	5	6	7	0	1	2	3	9	8
5	5	4	8	9	1	0	7	6	2	3
6	6	9	4	8	2	7	0	5	3	1
7	7	8	9	4	3	6	5	0	1	2
8	8	7	5	6	9	2	3	1	0	4
9	9	6	7	5	8	3	1	2	4	0

Table 2:

Corollary 3.4. *Let L be a nonassociative C-loop of order n with nucleus N of order m, then if for some positive integer t, 3^t divides n, then 3^t also divides m.* □

The next proposition confirms that there are indeed some even orders for which no nonassociative C-loop exists.

Proposition 3.5. *There is no nonassociative C-loop of order $2 \cdot 3^t$ for $t \geqslant 1$.*

Proof. n/m is not divisible by 3, hence $L/N(L)$ is of index at most 2, which is impossible by [14]. □

The following proposition states that there exist orders for which all nonassociative C-loops will be Steiner.

Proposition 3.6. *A nonassociative C-loop L of order $2p$ with p prime, is Steiner.*

Proof. Since L is nonassociative, $p > 2$. Let m be the order of $N(L)$. Since $N(L)$ is normal in L by [14], m divides $2p$. If $m = 2p$, $L = N(L)$ is a group. If $m = p$ then $N(L)$ is of index 2 in L, which is impossible by [14]. Similarly, by [14] $L/N(L)$ is Steiner. If $m = 2$ then $L/N(L)$ is Steiner of order p, which again is impossible. Thus $m = 1$ and L is Steiner. □

Example 3.7. The smallest nonassociative C-loop (size of nucleus = 1) is given in table 2. Since its order is $n = 10 = 2 \cdot 5$, it is also Steiner.

It is well known that there are two nonassociative C-loops of order 14. Being of order of the form $2p$ both are Steiner with nucleus of order 1.

Remark 3.8. Exploiting the results of Propositions 3.2, 3.5, and 3.6 can speed up automatic enumeration of C-loops. For example, we know by 3.2 that there is no nonassociative C-loop of order 18 , by 3.6 that C-loops of order 24 are all non-Steiner and by 3.5 that C-loops of order 22 are all Steiner.

Next we give the general forms of the nuclei of the nonassociative C-loops. Here p is an odd prime other than 3.

Order of C-loop	Admissible order of nucleus
$2 \cdot 3^k p,\ k \geqslant 1$	3^k
$2p$	1
$2^l,\ l \geqslant 4$	$1, 2, 2^2, \ldots, 2^{l-2}$
$2^l \cdot 3^k,\ l \geqslant 1, k \geqslant 1$	$2^h \cdot 3^k, 0 \leqslant h \leqslant l-2$
$2^2 p$	$1, 2, p$
$2p^2$	$1, p$
$2^k p,\ k > 2$	$2^h, 2^l p, 0 \leqslant h \leqslant k-1, 0 \leqslant l \leqslant k-2$
$2p^k,\ k > 2$	$p^l, 0 \leqslant l \leqslant k-1$
$2^2 p^2$	$1, 2, p, p^2, 2p$
$2^2 \cdot 3 \cdot p$	$3, 6, 3p$

As application of the above table we can give the orders of C-loops and the admissible orders of their corresponding nuclei in the following table.

C-loop	Nucleus	C-loop	Nucleus	C-loop	Nucleus
10	1	42	3	74	1
12	3	44	$1, 2, 11$	76	$1, 2, 19$
14	1	46	1	78	3
16	$1, 2, 4$	48	$3, 6, 12$	80	$1, 2, 4, 5, 8, 10, 20$
20	$1, 2, 5$	50	$1, 5$	82	1
22	1	52	$1, 2, 13$	84	$3, 6, 21$
24	$3, 6$	56	$1, 2, 4, 7, 14$	86	1
26	1	58	1	88	$1, 2, 4, 11$
28	$1, 2, 7$	60	$3, 6, 15$	90	$9, 18, 45$
30	3	62	1	92	$1, 2, 23$
32	$1, 2, 4, 8$	64	$1, 2, 4, 8, 16$	94	1
34	1	66	3	96	$3, 6, 12$
36	9	68	$1, 2, 7$	98	$1, 7$
38	1	70	$1, 5, 7$	100	$1, 2, 5$
40	$1, 2, 4, 5, 10$	72	$9, 18$		

4. Commutant of C-loops

The commutant of a loop is also known as the centrum, Moufang center or semi-center [8]. As discussed in [8], in a group, or even a Moufang loop, the commutant is a subloop, but this does not need to be the case in general. In [8], it has been proved that the commutant of a Bol loop of odd order is a subloop. In the following we discuss such a special case for the commutant of C-loops, which is not necessarily a subloop as the following example demonstrates:

Example 4.1. Consider the following nonassociative flexible C-loop of order 20, which has a commutant as $\{0, 1, 2, 3, 4, 5\}$ that is not a subloop.

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

We now investigate a condition under which the commutant of C-loop will be a subloop.

Proposition 4.2. *Let $C(L)$ be the commutator of a C-loop L. If every element in $C(L)$ has odd order then $C(L)$ is a subloop of L.*

Proof. Since $C(L)$ is has odd order by [14], then in fact, C(L) = Z(L). By [14] L is power-alternative, thus $C(L)$ is closed under powers. Now, let $a, b \in C(L)$ with $|a| = 2k + 1$. Then $a = a^{2k+2}$ is a square, hence in $N(L)$ again by [14]. The rest of the proof is clear from this observation. □

References

[1] **A. Beg**, *A Theorem on C-loops*, Kyungpook Math. J. **17** (1977), 91–94.

[2] **A. Beg**, *On LC-, RC-, and C-loops*, Kyungpook Math. J. **20**(2) (1980), 211–215.

[3] **F. Fenyves**, *Extra Loops I*, Publ. Math. Debrecen **15** (1968), 235–238.

[4] **F. Fenyves**, *Extra Loops II*, Publ. Math. Debrecen **16** (1969), 187–192.

[5] **E. G. Goodaire, E. Jespers and C. P. Milies**, *Alternative Loop Rings*, North-Holland Math. Studies, **184**, Elsevier.

[6] **M. K. Kinyon, K. Kunen and J. D. Philips**, *A generalization of Moufang and Steiner loops*, Algebra Universalis **48** (2002), 81–101.

[7] **M. K. Kinyon, Kyle Pula and P. Vojtechovsky**, *Admissible orders Of Jordan loops*, J. Combinatorial Designs **17** (2009), 103–118.

[8] **M. K. Kinyon, J. D. Phillips**, *Commutants of Bol loops of odd order*, Proc. Amer. Math. Soc. **132** (2004), 617–619.

[9] **M. K. Kinyon, J. D. Philips and P. Vojtechovsky**, *Loops of Bol-Moufang type with a subgroup of index* 2, Bul. Acad. Stiinte Repub. Mold. Mat. **3** (2005), 71–87.

[10] **M. K. Kinyon, J. D. Philips and P. Vojtechovsky**, *C-loops: extensions and constructions*, J. Algebra Appl. **6** (2007), 1–20.

[11] **G. P. Nagy and P. Vojtechovsky**, *LOOPS: Computing with quasigroups and loops in GAP, version 1.0.0*, http://www.math.du.edu/loops.

[12] **J. D. Phillips and P. Vojtechovsky**, *The varieties of loops of Bol-Moufang type*, Algebra Universalis **54** (2005), 259–271.

[13] **J. D. Phillips and P. Vojtechovsky**, *The varieties of quasigroups of Bol-Moufang type: An equational reasoning approach*, J. Algebra **293** (2005), 17–33.

[14] **J. D. Philips and P. Vojtechovsky**, *C-loops: an introduction*, Publ. Math. Debrecen **68** (2006), 115–137.

[15] **V. S . Ramamurthi and A. R. T. Solarin**, *On finite right central loops*, Publ. Math.Debrecen **35** (1988), 260–264.

[16] **J. Slaney**, *FINDER, finite domain enumerator: System description.* In Proc. of CADE-12, pp. 798–801, Springer, 1994.

[17] **J. Slaney and A. Ali**, *Generating loops with the inverse property.* In Proc. of ESARM 2008, pp. 55–66.

Received September 24, 2012

M. Shah, A. Ali
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mails: shahmaths_problem@hotmail.com, dr_asif_ali@hotmail.com

V. Sorge
School of Computer Science, The University of Birmingham, Edgbaston, Birmingham B15 2TT, UK
E-mail: v.sorge@cs.bham.ac.uk