Construction of mono-associative quasigroups

Mehtab Khan and *Amir Khan*

Abstract. We construct an infinite family of mono-associative quasigroups whose smallest member is of order 4, and an infinite family of non-commutative mono-associative quasigroups whose smallest member is of order 6. We also construct an infinite family of such quasigroups with left or two-sided identity.

Mono-associative quasigroups are quasigroups satisfying $x(xx) = (xx)x$ for all x. For more study on mono-associative quasigroups and loops we refer [1, 2, 3].

Let G and A be two multiplicative groups with neutral elements 1_g and 1_a respectively. We take a map $\mu : G \times G \to A$ and then define multiplication on $G \times A$ by

$$(g, a)(h, b) = (gh, a * b * \mu(g, h)), \quad \text{where } g, h \in G \text{ and } a, b \in A.$$

The resulting groupoid is clearly a quasigroup. It will be denoted by (G, A, μ).

In the following lemma we give a scheme to construct an infinite family of mono-associative quasigroups.

Lemma 1. *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is a mono-associative quasigroup if and only if*

$$\mu(g^2, g) = \mu(g, g^2), \quad \textit{for all } g \in G. \tag{1}$$

Proof. By definition the quasigroup (G, A, μ) is mono-associative quasigroup if and only if

$$\big((g, a)(g, a)\big)(g, a) = (g, a)\big((g, a)(g, a)\big).$$

This gives

$$(g^2, a^2 * \mu(g, g))(g, a) = (g, a)(g^2, a^2 * \mu(g, g))$$
$$(g^3, a^3 * \mu(g, g) * \mu(g^2, g)) = (g^3, a^3 * \mu(g, g) * \mu(g, g^2)).$$

Comparing both sides, we get (1). Hence the result follows. □

2010 Mathematics Subject Classification: 20M05.
Keywords: quasigroup, mono-associative quasigroup.

Proposition 1. *Let $n \geqslant 2$ be an integer. Let A be a cyclic group of order n, and $y \in A$ an element of order bigger than 1. Let $G = \{1, x\}$ be a multiplicative group of order 2 with neutral element e. Define $\mu : G \times G \to A$ by*

$$\mu(a,b) = \begin{cases} y & \text{if } (a,b) = (1,x),(x,1) \\ e & \text{otherwise.} \end{cases} \tag{2}$$

Then $Q = (G, A, \mu)$ is a non-associative, mono-associative quasigroup.

Proof. To show that $Q = (G, A, \mu)$ is mono-associative quasigroup, we must verify (1). It is easy to see that $Q = (G, A, \mu)$ is non-associative and commutative. □

Proposition 2. *Let $n \geqslant 2$ be an integer. Let A be a cyclic group of order n and $y \in A$ an element of order bigger than 1. Let $G = \{1, x, x^2\}$ be a multiplication group of order 3 with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(a,b) = \begin{cases} y & \text{if } (a,b) = (1,x^2),(x,x^2),(x^2,x) \\ e & \text{otherwise.} \end{cases} \tag{3}$$

Then $Q = (G, A, \mu)$ is a non-associative, mono-associative quasigroup with left identity $(1, e)$.

Proof. To show that $Q = (G, A, \mu)$ is mono-associative quasigroup, we must verify (1). Since $\big((x^2, e)(x, y)\big)(x^2, y) \neq (x^2, e)\big((x, y)(x^2, y)\big)$, $Q = (G, A, \mu)$ is non-associative. □

Analogously we can verify

Proposition 3. *Let $n \geqslant 2$ be an integer. Let A be a cyclic group of order n and $y \in A$ an element of order bigger than 1. Let $G = \{1, x, x^2\}$ be a multiplication group of order 3 with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(a,b) = \begin{cases} y & \text{if } (a,b) = (1,x^2),(x,1),(x,x^2),(x^2,x) \\ e & \text{otherwise.} \end{cases} \tag{4}$$

Then $Q = (G, A, \mu)$ is a non-associative, mono-associative quasigroup.

Proposition 4. *Let $n \geqslant 2$ be an integer. Let A be a cyclic group of order n and $y \in A$ an element of order bigger than 1. Let $G = \{e, a, b, c\}$ be the Klein 4-group with neutral element e. Define $\mu : G \times G \to A$ by*

$$\mu(g,h) = \begin{cases} y & \text{if } (g,h) = (a,b),(a,c),(b,c) \\ e & \text{otherwise.} \end{cases} \tag{5}$$

Then $Q = (G, A, \mu)$ is a non-associative, mono-associative quasigroup.

Example 1. The smallest group A satisfying the assumption of Proposition 1 is the 2-element cyclic group $\{e, y\}$. The construction of Proposition 1 gives rises to the smallest non-associative, commutative quasigroup of order 4.

$\cdot$	$(1,e)$	$(1,y)$	(x,e)	(x,y)
$(1,e)$	$(1,e)$	$(1,y)$	(x,y)	(x,e)
$(1,y)$	$(1,y)$	$(1,e)$	(x,e)	(x,y)
(x,e)	(x,y)	(x,e)	$(1,e)$	$(1,y)$
(x,y)	(x,e)	(x,y)	$(1,y)$	$(1,e)$

$=$

$\cdot$	1	2	3	4
1	1	2	4	3
2	2	1	3	4
3	4	3	1	2
4	3	4	2	1

Example 2. The smallest group A satisfying the assumption of Proposition 2 is the 2-element cyclic group $\{e, y\}$. The construction of Proposition 2 gives rises to the smallest non-associative non-commutative mono-associative quasigroup of order 6.

$\cdot$	$(1,e)$	(x,e)	(x^2,e)	$(1,y)$	(x,y)	(x^2,y)
$(1,e)$	$(1,e)$	(x,e)	(x^2,y)	$(1,y)$	(x,y)	(x^2,e)
(x,e)	(x,e)	(x^2,e)	$(1,y)$	(x,y)	(x^2,y)	$(1,e)$
(x^2,e)	(x^2,e)	$(1,y)$	(x,e)	(x^2,y)	$(1,e)$	(x,y)
$(1,y)$	$(1,y)$	(x,y)	(x^2,e)	$(1,e)$	(x,e)	(x^2,y)
(x,y)	(x,y)	(x^2,y)	$(1,e)$	(x,e)	(x^2,e)	$(1,y)$
(x^2,y)	(x^2,y)	$(1,e)$	(x,y)	(x^2,e)	$(1,y)$	(x,e)

Example 3. The smallest group A satisfying the assumption of Proposition 3 is the 2-element cyclic group $\{1, y\}$. The construction of Proposition 3 gives rises to the smallest non-associative non-commutative mono-associative quasigroup of order 6.

$\cdot$	$(1,e)$	(x,e)	(x^2,e)	$(1,y)$	(x,y)	(x^2,y)
$(1,e)$	$(1,e)$	(x,e)	(x^2,y)	$(1,y)$	(x,y)	(x^2,e)
(x,e)	(x,y)	(x^2,e)	$(1,y)$	(x,e)	(x^2,y)	$(1,e)$
(x^2,e)	(x^2,e)	$(1,y)$	(x,e)	(x^2,y)	$(1,e)$	(x,y)
$(1,y)$	$(1,y)$	(x,y)	(x^2,e)	$(1,e)$	(x,e)	(x^2,y)
(x,y)	(x,e)	(x^2,y)	$(1,e)$	(x,y)	(x^2,e)	$(1,y)$
(x^2,y)	(x^2,y)	$(1,e)$	(x,y)	(x^2,e)	$(1,y)$	(x,e)

Example 4. The smallest group A satisfying the assumption of Proposition 4 is the 2-element cyclic group $\{1, y\}$. The construction of Proposition 4 gives rises to the smallest non-associative non-commutative mono-associative quasigroup of order 8.

$\cdot$	$(1,e)$	(a,e)	(b,e)	(c,e)	$(1,y)$	(a,y)	(b,y)	(c,y)
$(1,e)$	$(1,e)$	(a,e)	(b,e)	(c,e)	$(1,y)$	(a,y)	(b,y)	(c,y)
(a,e)	(a,e)	$(1,e)$	(c,y)	(b,y)	(a,y)	$(1,y)$	(c,e)	(b,e)
(b,e)	(b,e)	(c,e)	$(1,e)$	(a,e)	(b,y)	(c,y)	$(1,y)$	(a,y)
(c,e)	(c,e)	(b,e)	(a,e)	$(1,e)$	(c,y)	(b,y)	(a,y)	$(1,y)$
$(1,y)$	$(1,y)$	(a,y)	(b,y)	(c,y)	$(1,e)$	(a,e)	(b,e)	(c,e)
(a,y)	(a,y)	$(1,y)$	(c,e)	(b,e)	(a,e)	$(1,e)$	(c,y)	(b,y)
(b,y)	(b,y)	(c,y)	$(1,y)$	(a,y)	(b,e)	(c,e)	$(1,e)$	(a,e)
(c,y)	(c,y)	(b,y)	(a,y)	$(1,y)$	(c,e)	(b,e)	(a,e)	$(1,e)$

Quasigroups constructed in the last three examples can be (respectively) identified with the following:

·	1	2	3	4	5	6
1	1	2	6	4	5	3
2	2	3	4	5	6	1
3	3	4	2	6	1	5
4	4	5	3	1	2	6
5	5	6	1	2	3	4
6	6	1	5	3	4	2

·	1	2	3	4	5	6
1	1	2	6	4	5	3
2	5	3	4	2	6	1
3	3	4	2	6	1	5
4	4	5	3	1	2	6
5	2	6	1	5	3	4
6	6	1	5	3	4	2

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

We verified the above three examples with the help of GAP package [4].

References

[1] **T.G. Jaiyéolá and J.O. Adêníran**, *New identities in universal Osborn loops*, Quasigroups and Related Systems, **17** (2009), 55 − 76.

[2] **T.G. Jaiyéolá and J.O. Adêníran**, *On another two cryptographic identities in universal Osborn loops*, Surv. Math. Appl. **5** (2010), 17 − 34.

[3] **M. Kinyon and I.M. Wanless**, *Loops with exponent three in all isotopes*, Internat. J. Algebra Comput. **25** (2015), 1159 − 1177.

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

Received April 20, 2017
Revised October 12, 2018

M. Khan
Department of Mathematics & Statistics, Bacha Khan University, Charsadda, Pakistan
E-mail: mehtabkhan85@gmail.com

A. Khan
Department of Mathematics and Statistics, University of Swat, Pakistan