PRINCIPAL LOOP-ISOTOPES OF QUASIGROUPS

B. F. BRYANT AND HANS SCHNEIDER

1. Introduction. If a quasigroup $(L, .)$ has finite order n, then there are n^2 principal loop-isotopes. Some of these n^2 loops may be isomorphic, and the main purpose of this paper is to obtain theorems that describe the isomorphism classes. Using these results and a computer, we have determined all the loops of order 6. These are listed (using the Fisher and Yates **(2)** designations) at the end of the paper.

A quasigroup $(L, .)$ is *isotopic* to a quasigroup $(M, \circ)$ provided there are three one-to-one mappings α, β, γ of L onto M such that x, $y \in L$ implies $x\alpha \circ y\beta = (x.y)\gamma$; if γ is the identity mapping, then we say $(L, .)$ is *principally isotopic* to $(M, \circ)$. Both isotopy and principal isotopy are equivalence relations.

If a quasigroup $(L, .)$ is isotopic to a quasigroup $(M, \circ)$, then there is a quasigroup $(L, \#)$ such that $(L, .)$ is principally isotopic to $(L, \#)$ and $(L, \#)$ is isomorphic to $(M, \circ)$ **(1)**. We are thus led to restrict our attention to the principal isotopes of a quasigroup $(L, .)$. Furthermore, we are primarily interested in those principal isotopes that are loops. The mappings α, β such that the quasigroup $(L, .)$ is principally isotopic to a loop $(L, \circ)$ under α and β are the mappings determined by $x\alpha = x.b$ and $y\beta = a.y$, where a, $b \in L$ **(1)**; for a fixed pair a and b, we shall denote the loop thus determined by $L(a, b)$, or if we need a symbol for the operation, we shall use $L(a, b, \circ)$. As usual, we write $a/b = c$ if and only if $a = c.b$, and $b\backslash a = d$ if and only if $a = b.d$. Thus the identity $(x.b) \circ (a.y) = x.y$ may be written in the equivalent form

$$x \circ y = (x/b).(a\backslash y).$$

2. Results.

THEOREM 1. *Let $(L, .)$ be a quasigroup. If $L(a, b, \circ)$ is isomorphic to $L(c, d, \#)$ under θ, then $L(e, f, \triangle)$ is isomorphic to $L[(e.b)\theta/d,\ c\backslash(a.f)\theta,\ \square]$ under θ. If $(L, .)$ is a loop, then*

$$(e.b)\theta/d = [e.(a\backslash c\theta^{-1})]\theta \text{ and } c\backslash(a.f)\theta = [(d\theta^{-1}/b).f]\theta.$$

Proof. The following identities hold:

$$(u.b) \circ (a.v) = u.v; \qquad u \circ v = (u/b).(a\backslash v); \qquad (u.d) \# (c.v) = u.v;$$
$$u \# v = (u/d).(c\backslash v); \qquad (u.f) \triangle (e.v) = u.v; \qquad u \triangle v = (u/f).(e\backslash y);$$
$$\{u.[c\backslash(a.f)\theta]\} \square \{[(e.b)\theta/d].v\} = u.v; \qquad (u \circ v)\theta = u\theta \# v\theta.$$

Received September 22, 1964.

If $x, y \in L$, then

$$\begin{aligned}[(x.f) \triangle (e.y)]\theta &= (x.y)\theta = [(x.b) \circ (a.y)]\theta = (x.b)\theta \# (a.y)\theta \\ &= [(x.b)\theta/d].[c\backslash(a.y)\theta] = \{[(x.b)\theta/d].[c\backslash(a.f)\theta]\} \square \{[(e.b)\theta/d].[c\backslash(a.y)\theta]\} \\ &= [(x.b)\theta \# (a.f)\theta] \square [(e.b)\theta \# (a.y)\theta] = [(x.b) \circ (a.f)]\theta \square [(e.b) \circ (a.y)]\theta \\ &= (x.f)\theta \square (e.y)\theta.\end{aligned}$$

Thus $L(e, f, \triangle)$ is isomorphic to $L[(e.b)\theta/d, c\backslash(a.f)\theta, \square]$.

If $(L, .)$ is a loop, then for each $x \in L, x/x = x\backslash x = 1$, where 1 is the identity. Hence

$$\begin{aligned}[e.(a\backslash c\theta^{-1})]\theta &= \{(e.b) \circ [a.(a\backslash c\theta^{-1})]\}\theta = [(e.b) \circ (c\theta^{-1})]\theta \\ &= (e.b)\theta \# c = [(e.b)\theta/d].(c\backslash c) = (e.b)\theta/d.\end{aligned}$$

Similarly, $c\backslash(a.f)\theta = [(d\theta^{-1}/b).f]\theta$.

Note that the first (second) member of $\{[e.(a\backslash c\theta^{-1})]\theta, [(d\theta^{-1}/b).f]\theta\}$ involves only the first (second) members of the pairs (a, b), (c, d), and (e, f); although the pair $[(e.b)\theta/d, c\backslash(a.f)\theta]$ is notationally simpler, it does not have this property.

If $(L, .)$ is a quasigroup, and if $L(a, b)$ is isomorphic to $L(c, d)$ under α and $(L(e, f)$ is isomorphic to $L(g, h)$ under β, then, by the above theorem, $L(c, d)$ is isomorphic to $L(i, j)$ under β for some $i, j \in L$; therefore $L(a, b)$ is isomorphic to $L(i, j)$ under $\alpha\beta$. Also, if $L(a, b)$ is isomorphic to $L(c, d)$ under θ, then $L(c, d)$ is isomorphic to $L(a, b)$ under θ^{-1}. Thus if $(L, .)$ is a quasigroup, then

$$G = \{\theta | L(a, b) \overset{\theta}{\approx} L(c, d) \quad \text{for some } a, b, c, d \in L\}$$

is a group. We shall call this group the group of the quasigroup $(L, .)$. The next theorem describes the effect on this group of isomorphisms and anti-isomorphisms of $(L, .)$.

THEOREM 2. *Let $(L, .)$ and $(M, \times)$ be quasigroups. If $(L, .)$ is isomorphic (anti-isomorphic) to $(M, \times)$ under θ, and if G is the group of $(L, .)$, then $\theta^{-1}G\theta$ is the group of $(M, \times)$.*

Proof. Let $\alpha \in G$, and let $L(a, b, \circ)$ be isomorphic to $L(c, d, \triangle)$ under α. We shall show that $M(a\theta, b\theta, \#)$ is isomorphic to $M(c\theta, d\theta, \square)$ under $\theta^{-1}\alpha\theta$.

$$\begin{aligned}[(x\theta \times b\theta) \# (a\theta \times y\theta)]\theta^{-1}\alpha\theta &= (x\theta \times y\theta)\theta^{-1}\alpha\theta = (x.y)\theta\theta^{-1}\alpha\theta = (x.y)\alpha\theta \\ &= [(x.b) \circ (a.y)]\alpha\theta = [(x.b)\alpha \triangle (a.y)\alpha]\theta = \{[(x.b)\alpha/d].[c\backslash(a.y)\alpha]\}\theta \\ &= [(x.b)\alpha/d]\theta \times [c\backslash(a.y)\alpha]\theta = \{[(x.b)\alpha/d]\theta \times d\theta\} \square \{c\theta \times [c\backslash(a.y)\alpha]\theta\} \\ &= \{[(x.b)\alpha/d].d\}\theta \square \{c.[c\backslash(a.y)\alpha]\}\theta = (x.b)\alpha\theta \square (a.y)\alpha\theta \\ &= (x.b)\theta\theta^{-1}\alpha\theta \square (a.y)\theta\theta^{-1}\alpha\theta \\ &= (x\theta \times b\theta)\theta^{-1}\alpha\theta \square (a\theta \times y\theta)\theta^{-1}\alpha\theta.\end{aligned}$$

If G' is the group of $(M, \times)$, then we have shown that $\theta^{-1}G\theta \subseteq G'$. But $(M, \times)$ is isomorphic to $(L, .)$ under θ^{-1}; hence $\theta G'\theta^{-1} \subseteq G$. Therefore $G' \subseteq \theta^{-1}G\theta$, and hence $G' = \theta^{-1}G\theta$.

The anti-isomorphism case is similar. In this case, if $\alpha \in G$ and $L(a, b)$ is isomorphic to $L(c, d)$ under α, then $M(b\theta, a\theta)$ is isomorphic to $M(d\theta, c\theta)$ under $\theta^{-1}\alpha\theta$.

$L(a, b)$ may be isomorphic to more than one principal loop-isotope of $(L, .)$ under a mapping θ. Theorems 3 and 4 are concerned with a description of this situation.

THEOREM 3. *If $(L, .)$ is a quasigroup, then $L(a, b, \circ)$ is isomorphic to $L(c, d, \#)$ under the identity map if and only if $c.b$ and $a.d$ are in $N_\mu[L(a, b, \circ)]$ (the middle nucleus of $L(a, b)$) and $a.b = c.d$.*

Proof. First suppose that $L(a, b, \circ)$ is isomorphic to $L(c, d\, \#)$ under the identity mapping; i.e. $x \circ y = x \# y$ for all $x, y \in L$. Since $a.b$ is the identity of $L(a, b, \circ)$ and $c.d$ is the identity of $L(c, d, \#)$, $a.b = c.d$. Now

$$\begin{aligned}
[x \circ (a.d)] \circ y &= \{(x/b).[a\backslash(a.d)]\} \circ y = [(x/b).d] \circ y = [(x/b).d] \# y \\
&= \{[(x/b).d]/d\}.(c\backslash y) = (x/b).(c\backslash y) = [(x/b).b] \circ [a.(c\backslash y)] \\
&= x \circ [a.(c\backslash y)] \\
&= x \circ \{(a.d) \# [c.(c\backslash y)]\} = x \circ [(a.d) \# y] = x \circ [(a.d) \circ y].
\end{aligned}$$

Hence $a.d \in N_\mu[L(a, b, \circ)]$.

Also

$$\begin{aligned}
x \circ [(c.b) \circ y] &= x \circ \{[(c.b)/b].(a\backslash y)\} = x \circ [c.(a\backslash y)] = x \# [c.(a\backslash y)] \\
&= (x/d).\{c\backslash[c.(a\backslash y)]\} = (x/d).(a\backslash y) = [(x/d).b] \circ [a.(a\backslash y)] \\
&= [(x/d).b] \circ y \\
&= \{[(x/d).d] \# (c.b)\} \circ y = [x \# (c.b)] \circ y = [x \circ (c.b)] \circ y.
\end{aligned}$$

Hence $c.b \in N_\mu[L(a, b, \circ)]$.

Conversely, suppose $c.b$ and $a.d$ are in $N_\mu[L(a, b, \circ)]$ and $a.b = c.d$. Recall that $a.b$ is the identity of $L(a, b, \circ)$.

$$\begin{aligned}
&[(a.d) \circ (c.b)] \circ [(a.d) \circ (c.b)] \\
&\quad = (a.d) \circ \{(c.b) \circ [(a.d) \circ (c.b)]\} = (a.d) \circ \{[(c.b) \circ (a.d)] \circ (c.b)\} \\
&\quad = (a.d) \circ [(c.d) \circ (c.b)] = (a.d) \circ [(a.b) \circ (c.b)] = (a.d) \circ (c.b).
\end{aligned}$$

Hence $(a.d) \circ (c.b) = a.b$. Thus

$$\begin{aligned}
[x \circ (a.d)] \circ [(c.b) \circ y] &= x \circ \{(a.d) \circ [(c.b) \circ y]\} \\
&= x \circ \{[(a.d) \circ (c.b)] \circ y\} = x \circ [(a.b) \circ y] = x \circ y = (x/b).(a\backslash y) \\
&= [(x/b).d] \# [c.(a\backslash y)] = \{[(x/b).b] \circ (a.d)\} \# \{(c.b) \circ [a.(a\backslash y)]\} \\
&= [x \circ (a.d)] \# [(c.b) \circ y].
\end{aligned}$$

Therefore $L(a, b, \circ)$ is isomorphic to $L(c, d, \#)$ under the identity mapping.

COROLLARY *If $(L, .)$ is a loop with identity 1, then $(L, .) = L(1, 1)$ is isomorphic to $L(c, d)$ under the identity mapping if and only if c and d are in the middle nucleus of $(L, .)$ and $c.d = 1$.*

THEOREM 4. *Let* $(L, .)$ *be a finite quasigroup,* G *the group of* $(L, .)$, *and* k *the order of* $N_\mu[L(a, b, \circ)]$. *If* $\theta \in G$, *then* $L(a, b, \circ)$ *is isomorphic under* θ *to* k *different principal loop-isotopes of* $(L, .)$.

Proof. We first prove the theorem for the identity mapping I. x can be selected in exactly k ways so that $x.b \in N_\mu[L(a, b, \circ)]$. Suppose that $x.b \in N_\mu[L(a, b, \circ)]$; then $(x.b) \circ \{a.[x\backslash(a.b)]\} = x.[x\backslash(a.b)] = a.b$. Since $a.b$ is the identity of $L(a, b, \circ)$ and $N_\mu[L(a, b, \circ)]$ is a group under $\circ$, $a.[x\backslash(a.b)]$ is the inverse of $x.b$ and is therefore in $N_\mu[L(a, b, \circ)]$. Hence, by Theorem 3, $L(a, b, \circ)$ is isomorphic under I to the k different principal loop-isotopes $L[x, x\backslash(a.b)]$, where $x.b \in N_\mu[L(a, b, \circ)]$.

Now let $\theta \in G$ and let m be the number of different principal loop-isotopes of $(L, .)$ to which $L(a, b)$ is isomorphic under θ. By Theorem 1,

$$L(a, b) \overset{\theta}{\approx} L(e, f)$$

for some $e, f \in L$. If

$$L(a, b) \overset{I}{\approx} L(c, d),$$

where $a \neq c$ or $b \neq d$, then, by Theorem 1,

$$L(e, f) \overset{I}{\approx} L[(e.b)/d, c\backslash(a.f)].$$

Hence

$$L(a, b) \approx L[(e.b)/d, c\backslash(a.f)]$$

under $\theta I = \theta$. Since $a \neq c$ or $b \neq d$, $a.f \neq c.f$ or $e.b \neq e.d$. Hence $c\backslash(a.f) \neq f$ or $(e.b)/d \neq e$. Thus $L[(e.b)/d, c\backslash(a.f)]$ is different from $L(e, f)$. It is also clear that if $d \neq d_1$ or $c \neq c_1$, then $(e.b)/d \neq (e.b)/d_1$ or $c\backslash(a.f) \neq c_1\backslash(a.f)$. Hence $m \geqslant k$.

Next suppose that

$$L(a, b) \overset{\theta}{\approx} L(e, f)$$

and

$$L(a, b) \overset{\theta}{\approx} L(g, h)$$

where $e \neq g$ or $f \neq h$. Then

$$L(e, f) \overset{\theta^{-1}}{\approx} L(a, b),$$

and hence, by Theorem 1,

$$L(g, h) \overset{\theta^{-1}}{\approx} L[(g.f)\theta^{-1}/b, a\backslash(e.h)\theta^{-1}].$$

Thus

$$L(a, b) \overset{I}{\approx} L[(g.f)\theta^{-1}/b, a\backslash(e.h)\theta^{-1}].$$

Since $a.b$ and $g.h$ are the identities of $L(a, b)$ and $L(g, h)$, respectively, we have $(a.b)\theta = g.h$. If $e \neq g$, then $e.h \neq g.h = (a.b)\theta$, and therefore $(e.h)\theta^{-1} \neq a.l$. Hence $a\backslash(e.h)\theta^{-1} \neq b$. If $f \neq h$, then $g.f \neq g.h = (a.b)\theta$, and therefore $(g.f)\theta^{-1} \neq a.b$. Hence $(g.f)\theta^{-1}/b \neq a$. Thus $L[(g.f)\theta^{-1}/b, a\backslash(e.h)\theta^{-1}]$ is different from $L(a, b)$. Also if $g \neq g_1$ or $h \neq h_1$, then $(g.f)\theta^{-1}/b \neq (g_1.f)\theta^{-1}/b$ or $a\backslash(e.h)\theta^{-1} \neq a\backslash(e.h_1)\theta^{-1}$. Hence $k \geqslant m$, and therefore $k = m$.

If $(L, .)$ is a finite quasigroup, and if $L(a, b)$ is isomorphic to $L(c, d)$, then the number of mappings under which $L(a, b)$ is isomorphic to $L(c, d)$ is the order of the group of automorphisms of $L(a, b)$. Then, by Theorem 4, we have the following theorem.

THEOREM 5. *If $(L, .)$ is a finite quasigroup, G the group of $(L, .)$, and $A(a, b)$ the group of automorphisms of $L(a, b)$, then the number of principal loop-isotopes of $(L, .)$ isomorphic to $L(a, b)$ is*

$$|G|\ |N_\mu[L(a, b)]|/|A(a, b)|.$$

Thus if $(L, .)$ is a loop of finite order n, G the group of $(L, .)$, and A the automorphism group of $(L, .)$, then a necessary and sufficient condition for all the loop-isotopes of $(L, .)$ to be isomorphic is

$$|G|\ |N_\mu(L, .)|/|A| = n^2.$$

Fisher and Yates **(2)** have given a member of each isotopy class for the quasigroups of order 6. There are 22 classes. The non-isomorphic loops of order 6 are then the non-isomorphic principal loop-isotopes of these 22 quasigroups. We have found these non-isomorphic principal loop-isotopes by using a computer. Fisher and Yates list only 17 quasigroups, I, II, . . . , XVII, since 12 of these are self anti-isomorphic and the other 5 are not. We use $A\,V$ to designate the quasigroup defined by $a \circ b = b.a$ where $\circ$ and . are the operations on $A\,V$ and V, respectively. We also use 1, 2, . . . , 6 rather than $a, b, \ldots, f$. With this notation, the 109 loops of order 6 are: I(1, 1), I(1, 2), I(1, 4), I(1, 6), I(2, 1), I(2, 2), I(2, 3), I(2, 4), I(2, 5), I(2, 6), AI(1, 1), AI(1, 2), AI(2, 1), AI(2, 2), AI(2,3), AI(4,1), AI(4,2), AI(4,3), AI(6,1), AI(6,2), II(1,1), II(1,2), II(1,4), II(1,6), II(2,1), II(2,2), II(2,3), II(2,4), II(2,5), II(2,6), III(1,1), III(1,2), III(1, 5), III(2, 1), III(2, 2), III(2, 3), III(2, 4), III(2, 5), III(2, 6), IV(1,1), IV(1, 2), IV(1, 3), IV(2, 1), IV(2, 2), IV(2, 3), IV(3, 1), IV(3, 2), IV(3, 3), IV(3, 4), IV(3, 5), IV(3, 6), V(1, 1), V(1, 2), V(1, 3), V(3, 1), V3, 2), V(3, 3), V(3, 5), AV(1, 1), AV(1, 3), AV(2, 1), AV(2, 3), AV(3, 1), AV(3, 3), AV(3, 4), VI(1, 1), VI(1, 2), VI(1, 3), VI(3, 1), VI(3, 3), VI(3, 4), VI(3, 5), VII(1, 1), VII(1, 2), VII(1, 3), VII(2, 1), VII(2, 2), VIII(1, 1), VIII(2, 1), VIII(2, 3), VIII(5, 1), AVIII(1, 1), AVIII(1, 2), AVIII(1, 4), AVIII(1, 5), IX(1, 1), IX(1, 2), IX(1, 3), IX(1, 5), X(1, 1), X(1, 2), XI(1, 1), XI(3, 1), XI(4, 1), AXI(1, 1), AXI(1, 3), AXI(1, 4), XII(1, 1), XII(1, 4), XII(1, 6), XIII(1, 1), XIV(1, 1), XV(1, 1), XV(2, 1), AXV(1, 1), AXV(1, 2), XVI(1, 1), XVI(1, 2), XVII(1, 1).

XIII is the cyclic group and XVII is S_3. XIV is the only other loop of order 6 that is isomorphic to all of its principal loop-isotopes.

The computing was done at the Oak Ridge National Laboratory, and the authors wish to express their appreciation to the members of the Mathematics Panel for their help in this project.

REFERENCES

1. R. H. Bruck, *A survey of binary systems* (Berlin–Göttingen–Heidelberg, 1958).
2. R. A. Fisher and F. Yates, *The* 6×6 *Latin squares*, Proc. Cambridge Philos. Soc., *30* (1934), 492–507.

Vanderbilt University and
University of Wisconsin