Realizations of Loops and Groups defined by short identities

A.D. Keedwell

Abstract. In a recent paper, those quasigroup identities involving at most three variables and of "length" six which force the quasigroup to be a loop or group have been enumerated by computer. We separate these identities into subsets according to what classes of loops they define and also provide humanly-comprehensible proofs for most of the computer-generated results.

Keywords: quasigroup identity, loop, group

Classification: 20N05

1. Introduction

In a recent paper [3], N.C. Fiala has investigated (with computer aid) which quasigroup identities involving at most three variables and with at most six variable occurrences imply that the quasigroup is necessarily a non-trivial loop or group. That author finds that there are 35 such "laws" which force the quasigroup to be a loop and that, of these, 16 force it to be a group. However, no proofs and no group or loop examples are given. We show here that the 35 laws[1] can be separated into subsets such that the members of each subset are realized by the same variety of loops or groups. We show also that some of the 35 loop and group laws listed in [3] are directly equivalent. Finally, for a sample of the laws listed in Theorem 4.1 of [3], we provide humanly comprehensible proofs that a quasigroup which satisfies one of these laws has to be a loop (or group).

For ease of reference, we label the identities listed in Table 1 below and in Theorem 4.1 of [3] in the form $La.b$, where a is the row and b is the column in which the identity $La.b$ occurs.

Following a suggestion of the referee, we begin by re-stating Theorem 4.1 of [3] as follows:

Theorem (see [3]). *There are exactly* 35 *quasigroup identities* (*up to renaming, cancelling, mirroring and symmetry*)[2] *connected by the product operation only and with at most six variable occurrences which imply that the quasigroup is*

[1]We frequently use the word "law" rather than "identity" to avoid confusion with the identity element of the loop or group which the identity induces.

[2]The statement in brackets is copied from the corresponding statement in Theorem 4.1 of [3].

necessarily a non-trivial loop or group. These 35 *identities are listed below in Table* 1.

$xx \cdot y = x \cdot yx$	$x[x(yy \cdot z)] = z$	$(xx)(y \cdot yz) = z$	$[x(x \cdot yy)]z = z$
$[(x \cdot xy)y]z = z$	$xx \cdot y = z \cdot yz$	$x[(xy \cdot z)y] = z^{(G)}$	$(xx)(y \cdot zy) = z$
$(xx \cdot yz)y = z$	$x \cdot xy = zz \cdot y$	$(xx \cdot y)z = zy$	$x(y \cdot xy) = zz$
$x(yx \cdot y) = zz$	$x[y(xy \cdot z)] = z^{(G)}$	$x(yx \cdot yz) = z^{(G)}$	$(xy)(x \cdot yz) = z^{(G)}$
$[x(y \cdot xy)]z = z$	$[(x \cdot yx)y]z = z$	$x(yx \cdot z) = yz^{(G)}$	$(xy)(x \cdot zy) = z^{(G)}$
$(xy \cdot xz)y = z^{(G)}$	$x(y \cdot xz) = zy^{(G)}$	$x(yy \cdot xz) = z$	$[x(y \cdot yx)]z = z$
$[(x \cdot yy)x]z = z$	$xy \cdot yz = xz^{(G)}$	$x[(yy \cdot z)x] = z$	$x(yy \cdot z) = zx$
$x \cdot yz = xy \cdot z^{(G)}$	$x(y \cdot zx) = yz^{(G)}$	$xy \cdot zx = yz^{(G)}$	$x \cdot yz = xz \cdot y^{(G)}$
$xy \cdot zx = zy^{(G)}$	$x \cdot yz = y \cdot zx^{(G)}$	$xy \cdot z = y \cdot zx^{(G)}$	

Table 1.

Those of the identities in Table 1 which, according to Theorem 4.2 of [3], imply that the quasigroup is a group are marked with a superscript (G).

2. Realization of group laws

We show in this section that, of the 16 laws which imply that a quasigroup satisfying one of them is a group, all those which are not balanced identities (as defined by Sade [4]) imply that the quasigroup is an abelian group of exponent two (that is, each of its non-identity elements has order two) and that, of the remaining four which are balanced, three imply that the group is abelian.

We begin with two lemmas, one new and one well-known.

Lemma 2.1. *Every unbalanced identity which involves three variables each occurring twice and which forces a quasigroup to be a loop or group also forces every non-identity element to have order two.*

Proof: Since the identity is unbalanced, one of the variables, say z, must occur twice on one side of the identity and not at all on the other side. On choosing each of the other two variables to be the identity element e, we get $zz = e$ for every choice of z. □

Lemma 2.2. *A group G all of whose non-identity elements have order two is abelian.*

Proof: Let $a, b \in G$. Then $ab \in G$ and so $(ab)(ab) = e$, whence $aababb = aeb$. That is, $ba = ab$. □

Theorem 2.3. *The twelve laws listed in Table* 2 *imply that a quasigroup which satisfies any one of them is an abelian group of exponent two.*

Proof: We assume that the computer-generated results of Fiala [3] are correct. (See Section 5 of this paper for humanly-comprehensible proofs of some of these results.) Since each of the laws listed in Table 2 is unbalanced, the result follows immediately from Lemmas 1 and 2 together. □

$x[(xy \cdot z)y] = z$	$x[y(xy \cdot z)] = z$	$x(yx \cdot yz) = z$	$(xy)(x \cdot yz) = z$
$x(yx \cdot z) = yz$	$(xy)(x \cdot zy) = z$	$(xy \cdot xz)y = z$	$x(y \cdot xz) = zy$
$xy \cdot yz = xz$	$x(y \cdot zx) = yz$	$xy \cdot zx = yz$	$xy \cdot zx = zy$

Table 2.

Theorem 2.4. *Each of the laws* $x \cdot yz = xy \cdot z$ ($L8.1$), $x \cdot yz = xz \cdot y$ ($L8.4$), $x \cdot yz = y \cdot zx$ ($L9.2$) *and* $xy \cdot z = y \cdot zx$ ($L9.3$) *implies that a quasigroup which satisfies it is a group. Each of the last three implies that the group is necessarily abelian.*

Proof: The first law is the associative law so any quasigroup which satisfies it is a group.

Since we are assuming (from [3]) that the associative law holds[3], the law $L8.4$ implies that $x(yz) = x(zy)$ and so $yz = zy$. Similarly, $L9.2$ implies that $x(yz) = (yz)x$ or that $xu = ux$ for arbitrary elements x, u. $L9.3$ likewise implies that $x(yz) = (yz)x$. □

3. Realization of loop laws

In this section, we separate the 19 laws of Table 1 which force a quasigroup to be a loop, but not necessarily a group, into five subsets according to the variety of loops which they define.

Again, we begin with a lemma.

Lemma 3.1. (a) *A loop* L *of exponent* 2 *which satisfies the relation* $u \cdot uv = v$ *for all* $u, v \in L$ *(left inverse property) is a left alternative loop; and conversely.*

(b) *One which satisfies the relation* $u \cdot vu = v$ *or the relation* $uv \cdot u = v$ *(crossed onverse property) is a medial alternative loop.*

Proof: (a) If a loop has exponent 2, $u \cdot uv = v \Leftrightarrow u \cdot uv = uu \cdot v$ since $uu = e$.

(b) The relation $u \cdot vu = v \Leftrightarrow vR_uL_u = v \Leftrightarrow R_uL_u = \mathrm{Id} \Leftrightarrow L_uR_u = \mathrm{Id} \Leftrightarrow vL_uR_u = v \Leftrightarrow uv \cdot u = v$ and so $u \cdot vu = uv \cdot u$. □

Theorem 3.2. *A loop defined by any one of the laws listed in Table* 3 *is a left alternative loop of exponent* 2 *or, equivalently, is a loop of exponent* 2 *with the left inverse property.*

Proof: We use Lemmas 2.1 and 3.1(a). For $L2.1$, $(x \cdot xy)y = e = yy$ so $x \cdot xy = y$. A similar argument can be used for $L6.4$. □

[3]The truth of this follows immediately from the fact that each of these laws is balanced. See Section 4.

$x[x(yy \cdot z)] = z$ $(L1.2)$	$(xx)(y \cdot yz) = z$ $(L1.3)$	$x(yy \cdot xz) = z$ $(L6.3)$
$[(x \cdot xy)y]z = z$ $(L2.1)$	$x \cdot xy = zz \cdot y$ $(L3.2)$	$[x(y \cdot yx)]z = z$ $(L6.4)$

Table 3.

Theorem 3.3. *A loop defined by any one of the laws listed in Table 4 is a crossed inverse property loop of exponent 2. Also, it satisfies the medial alternative law.*

Proof: We use Lemmas 2.1 and 3.1(b) and, for $L3.4, L4.1, L5.1, L5.2$, we use variants of the argument for $L2.1$ in Theorem 3.2. □

$(xx)(y \cdot zy) = z$ $(L2.4)$	$(xx \cdot yz)y = z$ $(L3.1)$	$x[(yy \cdot z)x] = z$ $(L7.3)$
$xx \cdot y = z \cdot yz$ $(L2.2)$	$x(y \cdot xy) = zz$ $(L3.4)$	$x(yx \cdot y) = zz$ $(L4.1)$
$[x(y \cdot xy)]z = z$ $(L5.1)$	$[(x \cdot yx)y]z = z$ $(L5.2)$	

Table 4.

Theorem 3.4. *Each of the laws* $[x(x \cdot yy)]z = z$ $(L1.4)$ *and* $[(x \cdot yy)x]z = z$ $(L7.1)$ *defines and is realized by any loop of exponent 2. Each of the laws* $(xx \cdot y)z = zy$ $(L3.3)$ *and* $x(yy \cdot z) = zx$ $(L7.4)$ *defines and is realized by any commutative loop of exponent 2.*

Proof: Use Theorem 4.1 of [3] and Lemma 2.1 above. □

Theorem 3.5. *The law* $xx \cdot y = x \cdot yx$ $(L1.1)$ *defines a variety of loops which are not necessarily of exponent 2. However, every loop of exponent 2 which has the crossed inverse property is a realization of this law.*

Proof: The existence of proper loops not of exponent 2 which satisfy $L1.1$ is shown by Figure 1 which gives the multiplication table of the smallest such loop. Moreover, every abelian group satisfies this law. □

Note that Sections 2 and 3 together account for, and provide realizations of the loops/groups defined by, all 35 of the laws listed in Table 1.

4. Further comments on the short identities which force a quasigroup to be a loop or group

We observe that, in fact, any commutative loop whose non-identity elements have order two and which satisfies $u \cdot uv = v$ for all $u, v \in Q$ is a realization of every one of the loops listed in Theorem 4.1 of [3] which is not a group. Such a loop $(L, \cdot)$ is a representation of a Steiner triple system S, where the elements of S are the non-identity elements of L and u, v, w is a triple of the system if $u \cdot v = w$ (and so $u \cdot w = v$ since $u \cdot uv = v$; also $w \cdot v = u$ since $w \cdot wu = u$). The smallest such loop which is not associative has order 10. The author is indebted to Michael Kinyon for the latter information and for supplying the multiplication table which we exhibit in Figure 2.

Figure 1 of the preceding section and the following information are also due to Kinyon.[4] The smallest *LIP*-loop (Theorem 3.2) of exponent two has order 6 and is shown in Figure 3. The smallest *CIP*-loop (Theorem 3.3) of exponent two has order 5 and is shown in Figure 4.

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

Figure 1

	1	2	3	4	5	6	7	8	9	0
1	1	2	3	4	5	6	7	8	9	0
2	2	1	4	3	6	5	9	0	7	8
3	3	4	1	2	7	0	5	9	8	6
4	4	3	2	1	8	9	0	5	6	7
5	5	6	7	8	1	2	3	4	0	9
6	6	5	0	9	2	1	8	7	4	3
7	7	9	5	0	3	8	1	6	2	4
8	8	0	9	5	4	7	6	1	3	2
9	9	7	8	6	0	4	2	3	1	5
0	0	8	6	7	9	3	4	2	5	1

Figure 2

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

Figure 3

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

Figure 4

We observe further that, of the 35 identities that force a quasigroup to be a loop or group, 18 are of the form $h(x,y,z) = z$, where $h(x,y,z)$ has one occurrence of z and two each of x and y. Of these, six take the form $[h(x,y)]z = z$ and so imply that $h(x,y) = e$. The remaining 12 can be separated into four sets of three equivalent identities, as we now show.

Remark. Surprisingly, the identities of the form LHS $= z$ listed in Theorem 4.1 of [3] are all of one of the forms $zL_{h(x,y)} = z$ or $zM_aM_bM_c = z$, where M_a is either L_a or R_a and each of a, b, c is one of x, y, xx, yy, xy or yx. None is of the form $zM_aM_b = z$, where each of a, b is as before or may involve three variable

[4]Kinyon obtained these results with computer aid, probably using mace4.

occurrences: for example, the identity $[x(yy)](zx) = z$ (which is not one of the 35 identities in Table 1) can be written $zR_xL_{x(yy)} = z$.

We look first at the identity $L1.2$. This is $x[x(yy \cdot z)] = z$ or we may write it in the form $zL_{yy}L_xL_x = z$. Therefore, $L_{yy}L_xL_x = \mathrm{Id}$. That is, $L_{yy}^{-1} = L_xL_x$ and $L_x^{-1} = L_{yy}L_x$. So, $L_xL_xL_{yy} = \mathrm{Id}$ and $L_xL_{yy}L_x = \mathrm{Id}$. Thence, $zL_xL_xL_{yy} = z$ and $zL_xL_{yy}L_x = z$. These are the identities $(yy)(x \cdot xz) = z$ (which is $L1.3$) and $x(yy \cdot xz) = z$ (which is $L6.3$). Thus, $L1.2 \Leftrightarrow L1.3 \Leftrightarrow L6.3$.

Next, we look at the identity $L2.4$. This is $(xx)(y \cdot zy) = z$ or we may write $zR_yL_yL_{xx} = z$. Therefore, $R_yL_yL_{xx} = \mathrm{Id}$. That is, $R_y^{-1} = L_yL_{xx}$ and $L_{xx}^{-1} = R_yL_y$. So, $L_yL_{xx}R_y = \mathrm{Id}$ and $L_{xx}R_yL_y = \mathrm{Id}$. Thence, $zL_yL_{xx}R_y = z$ and $zL_{xx}R_yL_y = z$. These are the identities $(xx \cdot yz)y = z$ (which is $L3.1$) and $y[(xx \cdot z)y] = z$ (which is $L7.3$). Thus, $L2.4 \Leftrightarrow L3.1 \Leftrightarrow L7.3$.

Similarly, the group identities $L2.3$, $L5.4$ and $L6.1$ are equivalent and so too are the group identities $L4.2$, $L4.3$ and $L4.4$, see Theorems 5.4 and 5.5 below.

There remains the question of finding humanly-comprehensible proofs that each of the identities listed in Theorem 4.1 is necessarily a loop (or group).

Since each of the identities $L8.1$, $L8.4$, $L9.2$ and $L9.3$ of Theorem 2.4 is a balanced identity in the sense of Sade [4] with a pair of variables separated on one side and not on the other, as required by Taylor's theorem (Taylor [5] and (earlier) Belousov [1], [2]), it follows that a quasigroup which satisfies any one of these is a group.

Also, for most of the other laws listed in Theorem 4.1 of [3], it is quite easy to show that a quasigroup which satisfies that law is unipotent but usually less easy to show that the element to which all squares are equal has to be an identity element.

We provide a few examples of such proofs.

5. Some proofs

Firstly, we consider two examples of laws of the form $[h(x,y)]z = z$.

Theorem 5.1. *A quasigroup* $(Q,\cdot)$ *which satisfies either of the identities* (A) $[x(x \cdot yy)]z = z$ ($L1.4$) *or* (B) $[x(y \cdot yx)]z = z$ ($L6.4$) *is necessarily a loop.*

Proof (A): Let $w \neq y$, where $w = x$ or $w = z$ if $(Q,\cdot)$ has only three elements. Then

$$(1) \qquad [x(x \cdot yy)]z = z = [x(x \cdot ww)]z.$$

Right cancelling z, we get $x(x \cdot yy) = x(x \cdot ww)$. Then, by left cancellation, we get $yy = ww = u$ say for all $y, w \in Q$ and so the quasigroup is unipotent and, in particular, $uu = u$. From (1), $[x(xu)]z = z$ for all $x, z \in Q$. Putting $x = u$ and using the fact that $uu = u$, this gives $uz = z$ and so u is a universal left identity. But, from the same equation, $x(xu)$ also is a universal left identity, so $x(xu) = u = xx$ by definition of u. Cancelling x, we get $xu = x$ and so u

is also a universal right identity. Therefore, the quasigroup is a loop and every non-identity element has order two.

Proof (B): Let $w \neq y$ as before, then we have

$$[x(y \cdot yx)]z = z = [x(w \cdot wx)]z. \tag{1}$$

If we cancel z on the right and then x on the left, we get

$$y \cdot yx = w \cdot wx \tag{2}$$

for all $w, x, y \in Q$. Put $w = f_x$ in (2), where (in Belousov's notation) f_v and e_v respectively denote the left and right local identities for the element v. We deduce that $y \cdot yx = x$ for all $x, y \in Q$. Therefore, from (1), $[xx]z = z$ for all $x, z \in Q$. It follows that $xx = yy = \cdots = u$ say is a universal left identity and that the quasigroup is unipotent. Thence, from (2), $y \cdot yu = u \cdot uu = uu = u = yy$. Cancelling y on the left, we get $yu = y$ and so u is also a universal right identity. Therefore, the quasigroup is a loop and every non-identity element has order two. $\square$

Secondly, we consider the four sets of three equivalent laws mentioned earlier.

We begin by providing humanly comprehensible proofs that a quasigroup which satisfies any one of identities $L1.2$, $L1.3$, $L6.3$ and $L2.4$, $L3.1$, $L7.3$ is a loop.

Theorem 5.2. *A quasigroup $(Q, \cdot)$ which satisfies any one of the equivalent identities $L1.2$, $L1.3$, $L6.3$ is a loop.*

Proof: We consider the identity $L1.3$: namely,

$$(yy)(x \cdot xz) = z. \tag{A}$$

Put $x = f_z$ in (A). Thence, $(yy)z = z$ and so $yy = f_z$ for all $y, z \in Q$. Thus, all squares are equal to f_z. Since z is arbitrary, f_z is a universal left identity, f say, and $xx = yy = \cdots = f$.

Now put $z = e_x$ in (A). We get $(yy)(xx) = e_x$ and so $e_x = ff = f$. That is, the right local identity of each element x is equal to the universal left identity f. Thus, f is a universal two-sided identity and $(Q, \cdot)$ is a loop in which every non-identity element has order two. Moreover, because $x \cdot xz = z$ from (A), the loop has the left inverse property. $\square$

Theorem 5.3. *A quasigroup $(Q, \cdot)$ which satisfies any one of the equivalent identities $L2.4$, $L3.1$, $L7.3$ is a loop.*

Proof: We consider the identity $L2.4$: namely,

$$(xx)(y \cdot zy) = z. \tag{B}$$

Put $z = f_y$ in (B). Thence, $(xx)(yy) = f_y$ for all $x, y \in Q$. We deduce that $(xx)(yy) = f_y = (ww)(yy)$ and so $ww = xx = u$ say.

From (B), $(xx)(x \cdot xx) = x$. That is, $u(xu) = x$ for all x.

Now put $y = u$ in (B) to get $(xx)z = z$. That is, $uz = z$ and so $u = f_z$ for all $z \in Q$. In other words, $u = ww = xx = \dots$ is a universal left identity. Therefore, from (B), $y \cdot zy = z$ for all y, z. Put $y = e_z$ in the last equality. This gives $e_z z = z$ and so $e_z = u$ for all z. Consequently, u is a universal right identity. Because $y \cdot zy = z$ for all y, z, $(Q, \cdot)$ is a loop with every non-identity element of order two and which satisfies the crossed inverse property. □

The next theorem provides a humanly comprehensible proof that each of the identities $L2.3$, $L5.4$ and $L6.1$ forces a quasigroup to be a group.

Theorem 5.4. *A quasigroup* $(Q, \cdot)$ *which satisfies any one of the identities* (A) $x[(xy \cdot z)y] = z$ ($L2.3$) *or* (B) $(xy)(x \cdot zy) = z$ ($L5.4$) *or* (C) $(xy \cdot xz)y = z$ ($L6.1$) *is a group.*

PROOF: The identity (A) can be written as $L_{xy}R_yL_x = \mathrm{Id}$ which implies that $R_yL_xL_{xy} = \mathrm{Id}$ and that $L_xL_{xy}R_y = \mathrm{Id}$; so the identities (A), (B) and (C) are equivalent.

The identity (C) implies that $(xy \cdot xz)y = z = (wy \cdot wz)y$ for all $w, x, y, z \in Q$. By right cancellation of y, we get

$$xy \cdot xz = wy \cdot wz. \tag{1}$$

In particular,

$$xx \cdot xx = wx \cdot wx. \tag{2}$$

Put $w = f_x$ in (2). This gives,

$$xx \cdot xx = xx \tag{3}$$

and so, from (2), $xx = wx \cdot wx$. For any $v \in Q$, there exists an element w such that $wx = v$ and so $xx = vv$ for every $v \in Q$. Let $xx = yy = \cdots = u$. Then, putting $y = z = x$ in the identity (C), we have $(xx \cdot xx)x = x$. That is, $(uu)x = x$ and so $ux = x$ for all $x \in Q$. Therefore, u is a universal left identity.

Put $x = u$ in the identity (C). Thence,

$$(yz)y = z \quad \text{for all} \quad y, z \in Q. \tag{4}$$

From the identity (B), we get $[(xy)(x \cdot zy)](xy) = z(xy)$ by multiplying on the right by xy. So, by (4),

$$x \cdot zy = z \cdot xy$$

for all $x, y, z \in Q$. This is a balanced identity[5] and so, by [5], $(Q, \cdot)$ is a group. It follows that the identity element u is two-sided[6] and that every non-identity element has order two. $\square$

Similarly, the next theorem provides a humanly comprehensible proof that each of the identities $L4.2$, $L4.3$ and $L4.4$ forces a quasigroup to be a group.

Theorem 5.5. *A quasigroup $(Q, \cdot)$ which satisfies any one of the identities* (A) $x[y(xy \cdot z)] = z$ ($L4.2$) *or* (B) $y(xy \cdot xz) = z$ ($L4.3$) *or* (C) $(xy)(x \cdot yz) = z$ ($L4.4$) *is a group.*

Proof: The identity (A) can be written as $L_{xy}L_yL_x = \mathrm{Id}$ which implies that $L_xL_{xy}L_y = \mathrm{Id}$ and that $L_yL_xL_{xy} = \mathrm{Id}$; so the identities (A), (B) and (C) are equivalent.

The identity (B) implies that $y(xy \cdot xz) = z = y(wy \cdot wz)$ for all $w, x, y, z \in Q$. By left cancellation of y, we get

$$xy \cdot xz = wy \cdot wz. \tag{1}$$

In particular,

$$xx \cdot xx = wx \cdot wx. \tag{2}$$

Put $w = f_x$ in (2). This gives,

$$xx \cdot xx = xx \tag{3}$$

and so, from (2), $xx = wx \cdot wx$. For any $v \in Q$, there exists an element w such that $wx = v$ and so $xx = vv$ for every $v \in Q$. Let $xx = yy = \cdots = u$. Then, putting $y = z = x$ in the identity (B), we have $x(xx \cdot xx) = x$. That is, $x(uu) = x$ and so $xu = x$ for all $x \in Q$. Therefore, u is a universal right identity.

Next, put $z = x = u$ in the identity (B). We get $y(uy \cdot u) = u$ or $y(uy) = u$. But $yy = u$ and so $uy = y$ for every $y \in Q$, whence u is also a universal left identity.

Put $x = u$ in the identity (B). Thence,

$$y(yz) = z \quad \text{for all} \quad y, z \in Q. \tag{4}$$

From the identity (C), we get $(xy)[(xy)(x \cdot yz)] = (xy)z$ by multiplying on the left by xy. So, by (4),

$$x \cdot yz = xy \cdot z$$

for all $x, y, z \in Q$. This is the associative law and so $(Q, \cdot)$ is a group. $\square$

---

[5] It appears to be different from those listed in Theorem 4.1 of [3]. In particular, it differs from $L9.2$ because the elements of the LHS and RHS are not in the same cyclic order.

[6] This can also be shown directly from the identity (B) because $(xx)(x \cdot xx) = x$ and $xx = u$ together imply that $u(xu) = x$ or that $xu = x$ for all $x \in Q$.

Finally, we consider a sample of the laws listed in Theorem 4.1 of [3] which are not of the form LHS $= z$ and are not balanced.

Theorem 5.6. *A quasigroup* $(Q,\cdot)$ *which satisfies either of the identities* (A) $(xx{\cdot}y)z = zy$ $(L3.3)$ *or* (B) $x(y{\cdot}xy) = zz$ $(L3.4)$ *is necessarily a loop. A quasigroup which satisfies* (C) $x(yx\cdot z) = yz$ $(L5.3)$ *is a group.*

Proof (A): Let $w \neq x$, where $w = y$ or $w = z$ if $(Q,\cdot)$ has only three elements as before. Then

$$(1) \qquad (xx\cdot y)z = zy = (ww\cdot y)z.$$

By right-cancelling z and then y in the equality $(xx\cdot y)z = (ww\cdot y)z$, we deduce that $xx = ww = u$ say for all $x, w \in Q$ and so the quasigroup is unipotent and, in particular, $uu = u$. Then, from (1),

$$(2) \qquad (uy)z = zy$$

for all $y, z \in Q$. Put $y = u$ in (2). Thence,

$$(3) \qquad uz = zu$$

for all $z \in Q$. Put $z = u$ in (2). We get $(uy)u = uy$. Since $uy = yu$ from (3), $(uy)u = yu$ and so, by right cancellation of u, $uy = y$. Therefore, u is a universal left identity. By virtue of (3), it is also a universal right identity. Thus, the quasigroup is a loop and every non-identity element has order two. Moreover, by (2), it is commutative.

Proof (B): Put $z = x$ in (B). We get $x(y\cdot xy) = xx$ and so

$$(1) \qquad y\cdot xy = x$$

for all x, y. Hence, from (B), $xx = zz = \cdots = u$ say, implying that the quasigroup is unipotent[7].

From (1), $x\cdot xx = x$. That is, $xu = x$ for all x, so u is a universal right identity.

Put $y = u$ and $z = x$ in (B). This gives $x(u\cdot xu) = xx$. Cancelling x on the left and replacing xu by x, we get $ux = x$ and so u is also a universal left identity.

Thus, the quasigroup is a loop whose non-identity elements have order two and which has the crossed inverse property (by virtue of the equality (1)).

Proof (C): Put $x = z$ in (C). This gives $z(yz\cdot z) = yz$. But, given $z \in Q$, we may choose $y \in Q$ such that $yz = w$ for any element $w \in Q$. Thus, $z(wz) = w$ for all $w, z \in Q$. We note that

$$z(wz) = w \Leftrightarrow R_z L_z = \mathrm{Id} \Leftrightarrow L_z R_z = \mathrm{Id} \Leftrightarrow (zw)z = w.$$

[7]The form of the given identity (B) itself shows that all squares are equal.

Now multiply (C) on the right by x. We get $[x(yx \cdot z)]x = (yz)x$ and so, using the equality just proved, $yx \cdot z = yz \cdot x$. This equality is a balanced identity and so $(Q, \cdot)$ is a group. $\square$

There exist similar humanly-comprehensible proofs for the remaining laws excepting only $L1.1$. The latter involves only two variables and requires a slightly different argument with which we end this paper.

Theorem 5.7. *A quasigroup $(Q, \cdot)$ which satisfies the identity $xx \cdot y = x \cdot yx$ ($L1.1$) is necessarily a loop.*

Proof: First put $y = f_x$ in $L1.1$. We get $xx \cdot f_x = xx$, so

$$f_x = e_{xx}. \tag{1}$$

Next, put $x = e_y$ in $L1.1$. We get $e_y e_y \cdot y = e_y y$, so

$$e_y e_y = e_y. \tag{2}$$

From (1) and (2), $f_x f_x = e_{xx} e_{xx} = e_{xx} = f_x$.

Now put $x = f_x$ in $L1.1$. We get $f_x f_x \cdot y = f_x \cdot y f_x$. That is, $f_x y = f_x \cdot y f_x$ whence, by left cancellation, $y = y f_x$. Thus, $f_x = e_y$ for all $x, y \in Q$.

Since both x and y are arbitrary, this implies that all left local identities are equal to all right local identities and so there is a universal two-sided identity. Consequently, Q is a loop. $\square$

Acknowledgment. The author wishes to thank the anonymous referee for a number of helpful suggestions which have led to an increase in the scope and usefulness of this paper.

References

[1] Belousov V.D., *Balanced identities in quasigroups* (in Russian), Mat. Sb. (N.S.) **70** (112) (1966), 55–97.

[2] Belousov V.D., *A theorem on balanced identities* (in Russian), Mat. Issled. **71** (1983), 22–24.

[3] Fiala N.C., *Short identities implying that a quasigroup is a loop or group*, Quasigroups Related Systems **15** (2007), 263–271.

[4] Sade A., *Entropie demosienne de multigroupoïdes et de quasigroupes*, Ann. Soc. Sci. Bruxelles, Sér. I, **73** (1959), 302–309.

[5] Taylor M.A., *A generalization of a theorem of Belousov*, Bull. Lond. Math. Soc. **10** (1978), 285–286.

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

(*Received* October 6, 2008, *revised* April 23, 2009)