When is it hard to show that a quasigroup is a loop?

A.D. Keedwell

Abstract. We contrast the simple proof that a quasigroup which satisfies the Moufang identity $(x \cdot yz)x = xy \cdot zx$ is necessarily a loop (Moufang loop) with the remarkably involved prof that a quasigroup which satisfies the Moufang identity $(xy \cdot z)y = x(y \cdot zy)$ is likewise necessarily a Moufang loop and attempt to explain why the proofs are so different in complexity.

Keywords: Moufang quasigroups, Moufang loops, identities of Bol-Moufang type

Classification: 20N05

1. Introduction

Kunen [6], [7] has discussed the question of when a quasigroup which satisfies a weak associative law is necessarily a loop and, in particular, he has solved this question for associative laws written with four variables, three of which are distinct. Following Fenyves [3], he has called the latter "laws of Bol-Moufang type".

Any such law (if duals are disregarded) is of one of the five forms:

(1) $(ab \cdot c)d = (ab)(cd)$ or
(2) $(ab \cdot c)d = a(bc \cdot d)$ or
(3) $(ab \cdot c)d = a(b \cdot cd)$ or
(4) $(a \cdot bc)d = (ab)(cd)$ or
(5) $(a \cdot bc)d = a(bc \cdot d)$,

where two of the variables a, b, c, d are the same.

Well-known examples of such laws are the Moufang identities. Again disregarding duals, there are two Moufang identities; one of each of the forms (4) and (3). For the first type, the demonstration that it is necessarily a loop is trivial but, for the second the proof is surprisingly complicated. (See [5], [6], [10].) The purpose of this paper is to elucidate the question "Why is this so?" by looking at each of the laws which force a quasigroup to be a loop.

2. History

Fenyves [3] was the first to introduce the term "identities of Bol-Moufang type" to describe weak associative laws involving three variables such that two of the variables occur once on each side, the third occurs twice on each side and the order in which the variables occur on each side is the same. He showed that there are 60 such laws but that, in the case of loops, 30 of them are equivalent to the full associative law (that is, they define the same variety of loops as does the full associative law: namely, the variety of groups). In this paper and making use of an earlier paper [2] concerned with a (then new) variety of loops which he called *extra loops*, Fenyves set out to determine, for any two loop identities of Bol-Moufang type, whether one of them implies the other or not. His results were not quite complete but, more recently, Phillips and Vojtěchovský [8] completed this task with the help, in some cases, of a computer-generated proof or counterexample as appropriate. Subsequently, Phillips and Vojtěchovský [9] carried out the same task for the variety of quasigroups: more precisely, they determined which quasigroup identities of Bol-Moufang type are equivalent to which others, which identities imply that a quasigroup satisfying such has a universal left identity (or, alternatively, a universal right identity), and which identities imply that a quasigroup has a universal two-sided identity and so is a loop. This latter work used computer-generated proofs quite extensively, not all of which were published in human-comprehensible form. Meanwhile, after the work of Fenyves and before that of Phillips and Vojtěchovský, Kunen [6], [7] had written the two papers already mentioned.

Note. In the two papers of Phillips and Vojtěchovský, these authors give names to a few of the Bol-Moufang identities which were not previously named. Also, in a recent paper of Drápal and Jedlička [1], the various identities which, in the case of loops, define Extra, Bol, or Moufang loops are given distinguishing names. Following a suggestion of the referee, we shall indicate names where they exist in square brackets.

3. Our investigation

Let us first point out that the first and last of the five forms listed in the Introduction immediately imply associativity except when $a = b$ or $c = d$ in the first case and except when $a = d$ or $b = c$ in the last. Moreover, in the first three of the special cases just mentioned, proper quasigroups exist which satisfy either one of these two forms so we shall only discuss form (5) in the case when $b = c$. Also, there exist proper quasigroups which satisfy the form (2) for all choices of a, b, c, d as the variables x, y, z (see Lemma 2.5 of [7]) so we shall not discuss this form either. (Note that one of these is the right Bol quasigroup which occurs when $b = d$.) We are left with laws of the forms (3) and (4) and one special case of the form (5).

Clearly, for a law of the form (4) above, it is easier to separate one variable and thence cancel it than it is for the third or fifth forms. Our first theorem below demonstrates this fact.

Theorem 1. *A quasigroup $(Q,\cdot)$ which satisfies the first Moufang [middle Moufang] identity* (A) $(x\cdot yz)x = xy\cdot zx$ *or its dual is a loop.*

Similarly, a quasigroup $(Q,\cdot)$ which satisfies one of the identities (B) $(x\cdot xy)z = xx\cdot yz$ *[left central] or (C) $(x\cdot yx)z = xy\cdot xz$ [numbered* (12) *in Fenyves* [3]*], or their duals, is a loop.*

Proof: Put $z = f_x$ in the middle Moufang identity, where (in Belousov's notation) f_u and e_u respectively denote the left and right local identities for the element u. We get $(x\cdot yf_x)x = xy\cdot f_x x = xy\cdot x$ by definition of f_x. Cancelling on the right by x, we get $x\cdot yf_x = xy$. Then, cancelling on the left by x, we have $yf_x = y$ for all $y\in Q$.

If f_u, f_v are left local identities for the elements $u,v\in Q$, then $yf_u = y$ and $yf_v = y$ for all $y\in Q$, so $yf_u = yf_v$ and thence $f_u = f_v$.

Thus, all left local identities coincide in an element f which is a universal right identity for the quasigroup (since $yf = y$ for all $y\in Q$). Moreover, by its definition, f is the left local identity for every element of Q. Therefore, f is a two-sided identity for $(Q,\cdot)$ and so $(Q,\cdot)$ is a loop.

For the identity (B), put $y = f_z$. We get $(x\cdot xf_z)z = xx\cdot f_z z = xx\cdot z$ by definition of f_z. Cancelling on the right by z, we get $x\cdot xf_z = xx$. Then, cancelling on the left by x, we have $xf_z = x$ for all $x\in Q$.

If f_u, f_v are left local identities for the elements $u,v\in Q$, then $yf_u = y$ and $yf_v = y$ for all $y\in Q$, so $yf_u = yf_v$ and thence $f_u = f_v$.

Thus, as before, all left local identities coincide in an element f which is a universal right identity for the quasigroup (since $yf = y$ for all $y\in Q$). Moreover, by its definition, f is the left local identity for every element of Q. Therefore in this case also, f is a two-sided identity for $(Q,\cdot)$ and so $(Q,\cdot)$ is a loop.

For the identity (C), put $x = f_z$. We get $(f_z\cdot yf_z)z = f_z y\cdot f_z z = f_z y\cdot z$ by definition of f_z. Cancelling on the right by z, we get $f_z\cdot yf_z = f_z y$. Then, cancelling on the left by f_z, we have $yf_z = y$ for all $y\in Q$.

The remainder of the proof is exactly the same as in the previous two cases. □

We note that each of the three laws considered in Theorem 1 is of the form (4).

Kunen [7] has shown that, excluding duals, there are nine weak associative laws of Bol-Moufang type with the property that a quasigroup which satisfies any one of them is a proper loop (that is, not a group). Five of these are of the form (4) considered in Theorem 1. The remaining two of these are (D) $(x\cdot yy)z = (xy)(yz)$ [numbered (32) in Fenyves [3]] and (E) $(x\cdot yz)y = (xy)(zy)$ [right extra for loops, see [1]]. We can apply the same techniques as in Theorem 1 to each of these but with less effective results.

In the case of (D), by putting $y = f_z$, we prove that f_z is a universal left identity. We get $(x\cdot f_z f_z)z = (xf_z)(f_z z) = xf_z\cdot z$ by definition of f_z. Cancelling on the right by z, we get $xf_zf_z = xf_z$ and so $f_zf_z = f_z$. Thence, $(xf_z)u = (x \cdot f_zf_z)u = (xf_z)(f_zu)$ and so, cancelling xf_z, $u = f_zu$ for all choices of the element u. Therefore, f_z is a universal left-identity. Call it f.

To show that f is also a universal right identity, Kunen [7] argues as follows:

Let u be the solution of the equation $u \cdot yy = f$. Putting $x = u$ in (D), we get

$$(\alpha) \qquad uy \cdot yz = (u \cdot yy)z = fz = z.$$

Putting $x = uy$ and $z = y$ in (D), we get

$$(uy \cdot y)(yy) = (uy \cdot yy)y = yy \ \ (\text{from } (\alpha) \text{ with } \ z = y) = f \cdot yy.$$

Cancelling yy, we have $uy \cdot y = f$. But, $uy \cdot yf = f$ from (α) with $z = f$.

Since the equation $uy \cdot v = f$ has a unique solution for v, $yf = y$ for all $y \in Q$. Consequently, f is a universal right identity and $(Q, \cdot)$ is a loop.

In the case of (E), by putting $z = f_y$, we prove that the left identity of each element is also its right identity. We get $(x \cdot yf_y)y = (xy)(f_yy) = xy \cdot y$ and so $x \cdot yf_y = xy$, giving $yf_y = y$. That is, $f_y = e_y$ for each element y.

To show that every element has the same two-sided local identity, Kunen argues as follows:

Put $x = y = f_z = e_z$ in (E). We get $f_zf_z \cdot ze_z = (f_z \cdot f_zz)e_z = ze_z = z$. That is, $f_zf_z \cdot z = z$ so $f_zf_z = f_z$ and each local identity is idempotent.

Let u be the solution of the equation $yu = e_x$. Putting $z = u$ in (E), we get $xy \cdot uy = (x \cdot yu)y = (xe_x)y = xy$. It follows that $uy = e_{xy}$.

Now put $x = z = u$ in (E). We get $uy \cdot uy = (u \cdot yu)y$ or, from above, $e_{xy}e_{xy} = (u \cdot e_x)y$. Since e_{xy} is idempotent, $uy = e_{xy} = e_{xy}e_{xy} = ue_x \cdot y$. Therefore, $ue_x = u$ and so $e_x = e_u$. Since $yu = e_x$, as y varies through Q so does u. Consequently, $e_x = e_u = e$ is a universal two-sided identity and $(Q, \cdot)$ is a loop.

The remaining four of the nine weak associative laws of Bol-Moufang type which force a quasigroup to be a loop are

(F) $(xy \cdot z)y = x(y \cdot zy)$, which is the second Moufang identity [right Moufang] and is of form (3);

(G) $(xy \cdot x)z = x(y \cdot xz)$, which is the dual of the second Moufang identity [left Moufang] and so need not be considered;

(H) $(xy \cdot z)x = x(y \cdot zx)$, which is the middle extra loop identity and is of form (3); and

(I) $(x \cdot yy)z = x(yy \cdot z)$ [middle nuclear square], which is the special case of form (5) that we mentioned earlier.

It is easy to see that a quasigroup $(Q, \cdot)$ which satisfies (I) is a loop because the identity (I) implies that all elements $u = yy$ which are squares lie in the middle nucleus of $(Q, \cdot)$. We appeal to the following lemma which was first proved by Garrison in Theorem 2.1 of [4]:

Lemma. *A quasigroup $(Q,\cdot)$ which has a non-empty middle nucleus N_μ is a loop.*

PROOF: Let $u \in N_\mu$. Then $xu \cdot z = x \cdot uz \dots (J)$ for all $x, z \in Q$. Put $x = f_u$ in (J). Thence, $uz = f_u(uz)$ and so $f_{uz} = f_u$. But, for fixed u, if v is any element of Q, there exists an element z such that $uz = v$. Therefore, $f_v = f_u$ for all $v \in Q$ and so there is a universal left identity f.

Similarly, by putting $z = e_u$ in (J), we find that $e_{xu} = e_u$ and so there is a universal right identity e. Then $f = fe = e$ and so $(Q,\cdot)$ is a loop. □

Kunen's arguments in [6] and [7] respectively to show that a quasigroup which satisfies either of the identities (F) or (H) is necessarily a loop are lengthy, involved and also dis-similar. The alternative argument of Izbash and Shcherbacov [5], [10] for the case of the identity (F), obtained independently, is even more lengthy.

Both these identities (and only these) take the form of an equality $(ab\cdot c)d = a(b\cdot cd)$ equating total associativity from the left to total associativity from the right and this seems to make the technique of substituting local identities particularly difficult to apply effectively.

The present author has tried to simplify these arguments but with very limited success. He offers the following marginal simplification for the case of the identity (F):

Theorem 2. *A quasigroup $(Q,\cdot)$ which satisfies the Moufang identity $(xy\cdot z)y = x(y\cdot zy)$ or its dual is a loop.*

PROOF: We first show that, for each element $y \in Q$, there exists an element $\overline{y}$ such that $y \cdot \overline{y}y = y$. Let e_y be the right local identity for y and let $\overline{y}$ be the solution for z of the equation $zy = e_y$. Then $y \cdot \overline{y}y = ye_y = y$, so $\overline{y}$ is the required element.

Put $z = \overline{y}$ in the above Moufang identity. We get $(xy \cdot \overline{y})y = xy$ and so $xy \cdot \overline{y} = x$ by cancelling y on the right. Since this result is valid for all $x \in Q$, we conclude that $\overline{y}$ is a right inverse for y. Thus, each element $y \in (Q,\cdot)$ has a right inverse y_R^{-1} which has the additional property that $y \cdot y_R^{-1}y = y$ as follows from its definition above. That is,

$$y_R^{-1}y = e_y. \tag{A}$$

Next, let a be a fixed element of Q. Then, putting $x = y = a$ and $z = f_a$ in the Moufang identity above, we get $(aa \cdot f_a)a = a(a \cdot f_a a) = a(aa)$. Multiplying on the right by a_R^{-1}, we get $[(aa \cdot f_a)a]a_R^{-1} = [a(aa)]a_R^{-1}$. That is,

$$aa \cdot f_a = [a(aa)]a_R^{-1}. \tag{B}$$

Again using the Moufang identity with $x = z = aa$ and $y = a_R^{-1}$, we have

$$[(aa \cdot a_R^{-1})(aa)]a_R^{-1} = (aa)(a_R^{-1}[(aa)a_R^{-1}]).$$

That is, $[a(aa)]a_R^{-1} = (aa)(a_R^{-1}a) = (aa)e_a$ using equation (A). Hence, from equation (B),

$$(aa)f_a = [a(aa)]a_R^{-1} = (aa)e_a.$$

It follows that $f_a = e_a$ by cancellation of aa. This proves that the left local identity and the right local identity of each element $a \in Q$ coincide.

Now put $x = y = f_a(= e_a)$ and $z = a$ in the Moufang identity. We get

$$(f_a f_a \cdot a)e_a = f_a(f_a \cdot ae_a) = f_a(f_a a) = a = ae_a.$$

That is, $f_a f_a \cdot a = a$ by right cancellation of e_a. We conclude that $f_a f_a = f_a$. Thus, the two-sided local identity for each element $a \in Q$ is an idempotent element.

Using the Moufang identity again, we get $(xf_u \cdot f_u)f_u = x(f_u \cdot f_u f_u) = x(f_u f_u) = xf_u$ and so, by right cancellation of f_u,

$$\text{(C)} \qquad xf_u \cdot f_u = x$$

for all elements $x, u \in Q$.

Now let a, b be two distinct elements of Q and put $w = f_b f_a$. Then $wf_a = f_b f_a \cdot f_a = f_b$ from equation (C). In the given Moufang identity, put $x = w$, $y = f_a$ and $z = f_b$. We get $(wf_a \cdot f_b)f_a = w(f_a \cdot f_b f_a)$ or $(f_b f_b)f_a = w(f_a \cdot w)$. But f_b is idempotent, so we have

$$\text{(D)} \qquad w = w \cdot f_a w.$$

Therefore, putting $y = w$ and $z = f_a$ in the Moufang identity we get

$$(xw \cdot f_a)w = x(w \cdot f_a w) = xw$$

by virtue of equation (D). Thus, by right cancellation of w, $xw \cdot f_a = x$ for any $x \in Q$. That is,

$$xw \cdot f_a = xf_a \cdot f_a$$

by equation (C). By right cancellation of f_a followed by left cancellation of x, we get $w = f_a$ or $f_b f_a = f_a = f_a f_a$ (since f_a is idempotent) and so $f_b = f_a$ by right cancellation of f_a again. We deduce that all local identity elements coincide in a universal identity element and so $(Q, \cdot)$ is a loop. □

It is interesting to note that the positions of the repeated variable are the same in the identities (E) and (F) and that the steps in the corresponding proofs follow the same order: (i) show that the left local identity of each element is equal to its right local identity; (ii) show that each such element is idempotent; (iii) show that all local identities coincide.

References

[1] Drápal A., Jedlička P., *On loop identities that can be obtained by nuclear identification*, submitted.

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

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

[4] Garrison G.R., *Quasi-groups*, Ann. Math. (2) **41** (1940), 474–487.

[5] Izbash V.I., Shcherbacov V.A., *On quasigroups with Moufang identity*, Abstracts of third Internat. Conf. in memory of M.I. Karbapolov, Krasnoyarsk, August 1993 (in Russian), pp. 134–135.

[6] Kunen K., *Moufang quasigroups*, J. Algebra **183** (1996), 231–234.

[7] Kunen K., *Quasigroups, loops, and associative laws*, J. Algebra **185** (1996), 194–204.

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

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

[10] Shcherbacov V.A., Izbash V.I., *On quasigroups with Moufang identity*, Bul. Acad. Stiinte Repub. Moldova Mat. 1998, no. 2, 109–116.

Department of Mathematics and Statistics, University of Surrey, Guilford, Surrey GU2 7XH, United Kingdom

(*Received* September 9, 2007, *revised* December 28, 2007)