Moufang Quasigroups
Kenneth Kunen

University of Wisconsin, Madison, WI 53706, U.S.A.
kunen@cs.wisc.edu
September 5, 1995

ABSTRACT

Each of the Moufang identities in a quasigroup implies that the quasigroup is a loop.

§1. Introduction. A quasigroup is a system $(G,·)$ such that $G$ is a non-empty set and $·$ is a binary function on $G$ satisfying $\forall x \forall y \exists z (xy = z)$ and $\forall x \forall y \exists z (yz = x)$. A loop is a quasigroup which has an identity element, 1, satisfying $\forall x (x1 = 1x = x)$. Quasigroups are studied not only in algebra, but also in combinatorics, where they are identified with Latin squares, and in projective geometry, where they are identified with 3-webs. For details and references to earlier literature, see the books [1, 2].

By results of Bol and Bruck (see [1], p. 115), the following four identities:

\begin{align*}
M1 : \forall xyz [(x(yz))x = (xy)(zx)] & \quad M2 : \forall xyz [(xz)(yx) = x((zy)x)] \\
N1 : \forall xyz [(xy)(z)y = x(y(zy))] & \quad N2 : \forall xyz [(yz)y = y(z(yx))] 
\end{align*}

are equivalent in loops; a loop satisfying these identities is called a Moufang loop. The purpose of this note is to show that every quasigroup satisfying any one of these identities is a loop (Theorems 2.2, 2.3), so that in fact these are equivalent in quasigroups. Observe that equations $M1, M2$ are mirrors of each other; that is, $M2$ is obtained by writing $M1$ backwards. Likewise, $N1, N2$ are mirrors of each other. Actually, [1] does not mention $M2$ explicitly, and just proves that $M1, N1, N2$ are equivalent, but any proof of $M1 \Leftrightarrow N1$ has a mirror which proves that $M2 \Leftrightarrow N2$.

Of course, a loop identity need not always imply its mirror. For example, the right and left Bol identities:

\begin{align*}
RBOL : \forall xyz [(xy)(yz)y = x((yz)y)] & \quad LBOL : \forall xyz [(y(zy))x = y(z(yx))] 
\end{align*}

are mirrors of each other, but, by an example of Zassenhaus (see [2], p. 46), there are 8-element loops satisfying one of these but not the other. In a quasigroup, equation $RBOL$ implies that there is a left identity element ([3] and Theorem 2.1); so, taking the mirror, $LBOL$ implies that there is a right identity, so that every quasigroup satisfying both $RBOL$ and $LBOL$ is a loop. However, by Robinson [6], there are non-loop quasigroups $(G, o)$ satisfying $RBOL$ but not $LBOL$; for example, let $G$ be any field of characteristic other than 2, and let $x o y = y - x$.

1 Author supported by NSF Grant CCR-9503445.
Our investigations have been aided by the automated deduction tool, OTTER, developed by McCune [5]. OTTER can prove theorems in full first-order logic, but it has been particularly useful in equational reasoning, where it can investigate substitutions much faster than a person can. Its proofs are long sequences of equations, and at first sight seem a bit inscrutable. However, as we showed in [4], by examining these proofs and trying different formulations of the input, one can often produce proofs which a person can easily verify by hand; we have done this in obtaining our proofs in §2.

§2. Proofs. We provide proofs for the three implications mentioned in §1. The first two are quite short. The first was given by Choudhury [3] in 1948, and we suspect that the second was also noticed before. We have not succeeded in finding a short proof of the third.

2.1. Theorem. ([3]) Every quasigroup satisfying RBOL has a left identity.

Proof. Fix any element $a$; then fix an $e$ such that $ea = a$. Applying RBOL, we have $(az)a = ((ea)z)a = e((az)a)$ for every $z$. Now, for every $y$ in a quasigroup, there is a $z$ such that $(az)a = y$, so $y = ey$ for every $y$. □

2.2. Theorem. Every quasigroup satisfying either $M1$ or $M2$ has a two-sided identity.

Proof. We assume $M1$; the proof from $M2$ is the mirror of this one. Fix any element $a$; then fix an $e$ such that $ae = a$. Applying $M1$, we have $(xa)x = (x(ae))x = (xa)(ex)$, and hence $x = ex$, for every $x$. So, $e$ is a left identity. Now, fix $b$ such that $be = e$. Applying $M1$ again, we have $(yb)e = (e(yb))e = (ey)(be) = ye$, and hence $yb = y$ for every $y$. So, $b$ is a right identity, and $b = eb = e$. □

2.3. Theorem. Every quasigroup satisfying either $N1$ or $N2$ has a two-sided identity.

Proof. We assume $N1$. For each $x$, define $j(x)$ and $k(x)$ by: $x \cdot j(x) = k(x) \cdot x = x$. In a loop, we would have $j(x) = k(x) = 1$ for all $x$.

First, we show that $j(x) = k(x)$ for all $x$. To see this, fix $a$, let $b = j(a)$ and $c = k(a)$, so $ab = ca = a$, and we want to show $c = b$. Now fix $d$ such that $da = b$. Applying $N1$, we have:

$$(ad)a = ((ca)d)a = c(a(da)) = c(ab) = ca = a \quad (\alpha)$$

but we can also cancel the $a$ to get:

$$ad = c \quad (\beta)$$

Applying $N1$, $(\alpha)$, and $(\beta)$:

$$ad = ((ad)a)d = a(d(ad)) = a(dc)$$

and we cancel to get:

$$dc = d \quad (\gamma)$$
Applying \( N1, (\beta), \) and \((\gamma)\):

\[
((xd)a)d = x(d(ad)) = x(dc) = xd
\]

Since \( \forall y \exists x(xd = y) \), we have, for every \( y \):

\[
(ya)d = y \tag{\delta}
\]

Applying \( N1, (\delta) \), and the definition of \( c \):

\[
(aa)c = [[[((aa)c)a] \cdot d] = [a(a(ca)))] \cdot d = (a(aa))d \tag{\epsilon}
\]

Applying \( N1, (\delta) \) (with \( y = a \)), and the definition of \( d \):

\[
(a(aa))d = (((aa)d) (aa)) = (aa) (d((aa) d)) = (aa)(da) = (aa)b \tag{\zeta}
\]

By \( (\epsilon) \) and \( (\zeta) \), we have \( (aa)c = (aa)b \), so \( c = b \), as claimed.

So, we have, for all \( x \):

\[
x \cdot j(x) = j(x) \cdot x = x \tag{1}
\]

We now show:

\[
 j(x) \cdot j(x) = j(x) \tag{2}
\]

To see this, apply \( N1 \) and (1) to get

\[
x = ((j(j(x)) \cdot j(x)) \cdot x) \cdot j(x) = j(j(x)) \cdot (j(x) \cdot (x \cdot j(x))) = j(j(x)) \cdot x
\]

Then \( j(j(x)) = j(x) \) follows from \( j(j(x)) \cdot x = x = j(x) \cdot x \), and then \( j(x) \cdot j(x) = j(x) \)

follows, since \( j(j(x)) \cdot j(x) = j(x) \) by (1).

Next, we show:

\[
 (x \cdot j(y)) \cdot j(y) = x \tag{3}
\]

To see this, apply \( N1 \) and (2):

\[
 ((x \cdot j(y)) \cdot j(y)) \cdot j(y) = x \cdot (j(y) \cdot (j(y) \cdot j(y))) = x \cdot j(y)
\]

and now cancel the \( j(y) \).

Finally, we show that \( j(x) \) is a constant, which must then be a two-sided identity by (1). To see this, we fix elements \( a, b \), and show \( j(a) = j(b) \). Let \( p = j(a)j(b) \). Note that \( pj(b) = j(a) \) by (3). Applying \( N1 \) and (2),

\[
p = j(a) \cdot j(b) = (j(a) \cdot j(a)) \cdot j(b) = ((p \cdot j(b)) \cdot j(a)) \cdot j(b) = p \cdot (j(b) \cdot (j(a) \cdot j(b))) = p \cdot (j(b) \cdot p)
\]

Using this with \( N1 \) and (3), we have for any \( x \):

\[
 ((x \cdot p) \cdot j(b)) \cdot p = x \cdot (p \cdot (j(b) \cdot p)) = x \cdot p = ((x \cdot j(b)) \cdot j(b)) \cdot p
\]

Cancelling, \( j(b) = p = j(a)j(b) \). Since also \( j(b) = j(b)j(b) \) by (2), we have \( j(a) = j(b) \). \( \square \)
References