Quasigroups, Loops, and Associative Laws

Kenneth Kunen [1]
University of Wisconsin, Madison, WI 53706, U.S.A.
kunen@math.wisc.edu

March 15, 1996

ABSTRACT

We investigate the question of which weakenings of the associative law imply that a quasigroup is a loop. In particular, we completely settle the question for all laws of "Bol – Moufang type" (those written with four variables, three of which are distinct).

§**1. Introduction.** A *quasigroup* is a system $(G, \cdot)$ such that G is a non-empty set and $\cdot$ is a binary function on G satisfying $\forall xz \exists! y(xy = z)$ and $\forall yz \exists! x(xy = z)$. A *loop* is a quasigroup which has an identity element, 1, satisfying $\forall x(x1 = 1x = x)$. See the books [1, 2, 9] for background and references to earlier literature.

A *group* is, by definition, an associative loop. As is well-known, every quasigroup satisfying the associative law has an identity element, and is hence a group. In this paper we consider weakenings of associativity which also imply that a quasigroup is a loop, even though many of these weakenings do not imply the full associative law.

For example, consider the four Moufang identities:

$$M1: \ (x(yz))x = (xy)(zx) \qquad M2: \ (xz)(yx) = x((zy)x)$$
$$N1: \ ((xy)z)y = x(y(zy)) \qquad N2: \ ((yz)y)x = y(z(yx))$$

As usual, equations written this way with variables are understood to be universally quantified. We showed in [6] that every quasigroup satisfying any of these is a loop; hence, by much earlier results of Bol and Bruck (see [1], p. 115), these four identities are equivalent in quasigroups, even though the quasigroups satisfying these identities (the Moufang loops) are not necessarily groups.

Definition. A *weak associative law* is an equation of the form $\alpha = \beta$, where for some variables, $V_1, V_2, \ldots, V_n$, (not necessarily distinct), α and β are both associations of the product $V_1 V_2 \cdots V_n$. We call n the *size* of the equation. The law is *non-trivial* iff α is not the same as β.

For example, the Moufang identities are weak associative laws of size four. All weak associative laws of size one and two are trivial. For size three, besides the trivial laws and the full associative law, there are three laws written with two distinct variables – the flexible law and the right and left alternative laws:

$$FLEX: x(yx) = (xy)x \qquad RALT: x(yy) = (xy)y \qquad LALT: y(yx) = (yy)x$$

[1] Author supported by NSF Grant CCR-9503445.

In §2, we point out that none of these three implies that a quasigroup is a loop, although any two of these together do. We also show that there is a single law of size four with two distinct variables which implies that a quasigroup is a loop.

Note that we need never consider weak associative laws written with just one variable, such as $(xx)x = x(xx)$ or $(xx)(xx) = x((xx)x)$. It is easy to construct a three-element non-loop quasigroup which satisfies $xx = x$, and is hence *power-associative* (that is, satisfies *all* one-variable associative laws).

We do not know of a simple criterion for telling which weak associative laws imply that a quasigroup is a loop, and we do not even know if this problem is decidable. In §3, we completely settle the problem for what Fenyves [4] called "identities of Bol – Moufang type". These are the ones of size four which have three distinct variables. They include the Moufang laws, as well as the Bol laws and the extra loop identities. After some preliminary reductions, discussed in §§2,3, there are 20 cases to consider.

As in [6], our investigations have been aided by the automated deduction tool, OTTER, developed by McCune [7]. This has been very useful in establishing that one equation implies another. Then, following the pattern in [5,6], we examined these proofs and converted them to the human-readable form presented here. In addition, we used the tools FINDER, programmed by Slaney [11], and MACE, programmed by McCune [8], to produce finite counter-examples. The output to these programs is simply a multiplication table, although by examining these tables, we have recognized them as isotopes of familiar groups, and have presented them that way in this paper.

§**2. Preliminary results.** This section describes some general facts to set the stage for the detailed analysis in the next section.

In most cases where we show that an equation does not imply that a quasigroup is a loop, the counter-example will be a group isotope of a particularly simple form. We introduce some notation for these.

Definition. If p is a prime and $0 < a, b < p$, let $I(a, b, p)$ be the structure $\mathbb{Z}_p$, with a product operation $\circ$ defined by: $x \circ y = ax + by$.

2.1. Lemma. $I(a, b, p)$ is a quasigroup, and is not a loop unless $a = b = 1$.

The search for a counter-example of this form reduces to elementary algebra. For example, say we want a non-loop quasigroup satisfying $((xx)y)z = x(x(yz))$. For this to be valid in $I(a, b, p)$, the coefficients of x, y, z yield three equations which a, b must satisfy: $aaa + aab = a + ba$, $ab = bba$, and $b = bbb$. The last two reduce to $b = 1$, whence the first becomes $a^3 + a^2 = 2a$, which has the solution $a = 3$ in $\mathbb{Z}_5$, so our counter-example is $I(3, 1, 5)$. We have used this type of example elsewhere [5] to obtain an easily described class of quasigroups.

Unfortunately, such simple examples do not always suffice. For example, the right alternative law, $RALT$, is not true in any $I(a, b, p)$ unless $a = b = 1$, although it is easy to describe a non-loop quasigroup satisfying $RALT$ (Lemma 2.3 below).

The *mirror* of an equation is obtained by writing it backwards. For example, $M1, M2$ in the Introduction are mirrors of each other as are $N1, N2$, and $LALT, RALT$. It happens that $M1, M2, N1, N2$ are all equivalent in quasigroups, but $LALT$ and $RALT$ are not

equivalent, even in loops. The flexible law, $FLEX$, is its own mirror. Of course, the mirror of a theorem is a theorem; for example, once we show (see Lemma 2.3) that there is a non-loop quasigroup satisfying $RALT$, the mirror of this quasigroup is a non-loop quasigroup satisfying $LALT$. Applying mirroring, we can often cut in half the number of cases we need to consider.

First, let us dispense with the laws of size three.

2.2. Lemma. In any quasigroup:

1. $RALT$ implies there is a right identity.
2. $LALT$ implies there is a left identity.
3. $FLEX$ plus either a right or a left identity implies that there is a two-sided identity.
4. Any two of $RALT, LALT, FLEX$ implies that there is a two-sided identity.

Proof. (4) is immediate from $(1-3)$. For (1), assume $RALT$, and fix a, b with $ab = a$. Then $a(bb) = (ab)b = ab$, so $bb = b$. Then, for any x, $(xb)b = x(bb) = xb$, so $xb = x$. Thus, there is a right identity. The proof of (2) is the mirror of this. For (3), say b is a right identity. Then, for any x, $x(bx) = (xb)x = xx$, so $bx = x$, so b is also a left identity. □

2.3. Lemma. There are non-loop quasigroups satisfying each of $RALT$, $LALT$, $FLEX$.

Proof. For $FLEX$, use $I(2,2,3)$. For $RALT$, use $\mathcal{G} = (\mathbb{Z}_6, \circ)$, where $x \circ y = x + f(y)$, where f is defined by the following table:

y	:	0	1	2	3	4	5
$f(y)$	:	0	4	5	3	1	2
$y \circ y = y + f(y)$	:	0	5	1	0	5	1

Since f is a bijection, $\mathcal{G}$ is a quasigroup. $RALT$ follows from $f(y \circ y) = f(y) + f(y)$, which is easily checked from the table. $\mathcal{G}$ is not a loop because 0 is a right identity (since $f(0) = 0$), but not a left identity. □

Let us now turn to laws of size greater than three. Informally, one would expect that the more distinct variables one allows, the stronger a law can be. As pointed out in the Introduction, we need not consider laws with just one variable. At the other extreme, consider the case where all variables are distinct, such as $(w(xy))z = (wx)(yz)$.

2.4. Lemma. If $\alpha = \beta$ is a non-trivial weak associative law of size n, and with n distinct variables, then every *loop* satisfying $\alpha = \beta$ is a group.

Proof. Induct on n. It is trivial for $n = 3$, and for $n > 3$, we may always replace one of the variables by 1, and then apply the Lemma for $n - 1$. □

This lemma is not true for quasigroups, however.

2.5. Lemma. There are non-loop quasigroups satisfying each of the two mirrors, $(w(xy))z = w(x(yz))$ and $((zy)x)w = z((yx)w)$.

Proof. Use $I(1,2,3)$ and $I(2,1,3)$, respectively. □

Note that these two equations can be weakened to the left and right Bol identities by setting $w = y$, and Robinson [10] already showed that neither of the Bol identities implies

that a quasigroup is a loop. It is not hard to see that every other non-trivial four variable law of size four implies that a quasigroup is a loop, and hence a group by Lemma 2.4.

Now, no two-variable weak associative law of any size can imply that a loop is a group, since every Moufang loop satisfies all of these laws together (by Moufang's Theorem). "Most" single two-variable laws of various sizes fail to imply that a quasigroup is a loop (e.g., $FLEX$ and $RALT$ and $LALT$ all fail). However there are exceptions, as we show next. First, a preliminary definition:

Definition. In a quasigroup, define the functions j and k by: $x \cdot j(x) = k(x) \cdot x = x$.

2.6. Lemma. If $j(x)$ is a constant, then this constant is a right identity. If $k(x)$ is a constant, then this constant is a left identity.

Lemmas about j and/or k turn out to be convenient preliminary steps in proving that a quasigroup is a loop. Examples of this technique are the next lemma and two of the proofs in §3. Another example is the proof in [6] that $N1$ or $N2$ imply that a quasigroup is a loop (the proofs from $M1$ or $M2$ are trivial exercises).

2.7. Lemma. Every quasigroup satisfying either of the mirrors $((xy)x)y = (xy)(xy)$ or $(yx)(yx) = y(x(yx))$ is a loop.

Proof. We argue from $((xy)x)y = (xy)(xy)$.

First, we show that $k(x)\,k(x) = k(x)$. To see this, fix any a, and then fix c such that $ac = k(a)$. Then

$$k(a) = ac = (k(a) \cdot a)c = ((ac)a)c = (ac)(ac) = k(a)\,k(a)$$

Next, we show that $k(x)$ is a constant. To see this, we fix a, b and prove $k(a) = k(b)$. Fix d such that $k(b) = ad$. Then

$$(k(b)\,a)d = ((ad)a)d = (ad)(ad) = k(b)\,k(b) = k(b) = ad$$

By cancelling, we get $k(b)\,a = a$. Since also $k(a)\,a = a$, we have $k(a) = k(b)$.

So, we have $k(x) = e$, a left identity. To show that e is a right identity, note that for any y

$$(ye)y = ((ey)e)y = (ey)(ey) = yy$$

We then cancel to get $ye = y$. □

§3. Size Four Laws with Three Distinct Variables. Although we see no general theorem here, we can organize the presentation somewhat by grouping the laws according to their syntactic form.

Every term written with four variables (not necessarily all distinct) is of one of three basic types, which we shall label as follows:

$T13$: $x \cdot \gamma$, where γ has three variables

$T31$: $\gamma \cdot x$, where γ has three variables

$T22$: $\gamma \cdot \delta$, where γ, δ each have two variables

At first, it would seem that these lead to nine different forms of equations between four variable terms, but in fact we need only consider two. We never need to consider equations of the form $T13 = T13$, since in a quasigroup, $x \cdot \gamma = x \cdot \delta$ is equivalent to $\gamma = \delta$, which has size 3 and has been dealt with in §2. Likewise, we need not consider equations of the form $T31 = T31$, and the only equation of the form $T22 = T22$ is trivial. So, we need only consider equations between two different types of terms, and obviously, it doesn't matter which one we write on the left of the $=$, so we have three, not six, forms of equations. Furthermore, the mirror of an equation of the form $T13 = T22$ is of form $T31 = T22$, so we need only consider equations of the form $T31 = T22$ and $T31 = T13$.

Now, a product of three variables can be associated in two ways, so that the two basic forms of equations can be organized into six sub-forms as follows:

$$\begin{array}{rcrcl}
T31L = T22 & : & ((V_1V_2)V_3)V_4 & = & (V_1V_2)(V_3V_4) \\
T31R = T22 & : & (V_1(V_2V_3))V_4 & = & (V_1V_2)(V_3V_4) \\
T31L = T13L & : & ((V_1V_2)V_3)V_4 & = & V_1((V_2V_3)V_4) \\
T31L = T13R & : & ((V_1V_2)V_3)V_4 & = & V_1(V_2(V_3V_4)) \\
T31R = T13L & : & (V_1(V_2V_3))V_4 & = & V_1((V_2V_3)V_4) \\
T31R = T13R & : & (V_1(V_2V_3))V_4 & = & V_1(V_2(V_3V_4))
\end{array}$$

Since we are looking at equations with three distinct variables, there are six possibilities for choosing the two variables from $\{V_1, V_2, V_3, V_4\}$ which are to be identical, so that each of these sub-forms yields six equations, obtained by replacing V_1, V_2, V_3, V_4 by one of the following sequences of variables:

$$xxyz, xyxz, xyzx, xyyz, xyzy, xyzz$$

Furthermore, we can immediately discard the two sub-forms $T31L = T13L$ and $T31R = T13R$ by Lemma 2.5. So, we need only consider four sub-forms under each of six substitutions, yielding 24 equations, which we list below. Actually, there are only 20, since the mirror of a $T31L = T13R$ is of the same sub-form $T31L = T13R$, and may or may not be an identical axiom, depending on the variables substituted. Still, to make our table more readable, we have listed all 24 in Table I. Under the heading "Loop?", we have listed "yes" or "no" depending on whether or not it implies that a quasigroup is a loop.

These 24 are all among the "60 identities of the Bol – Moufang type" considered by Fenyves [4]. Our list is a proper subset of his, since we are discarding some laws which we have already seen do not imply a quasigroup is a loop, and we are discarding some mirrors. There seems to be no natural way of numbering these laws, so we have simply copied his numbers in our table, along with the name of the law if it has one. The only names which are conspicuously missing are the Bol identities, which have already been discarded.

Some further remarks on our name labels. $M1, M2, N1, N2$ are the Moufang axioms, as in the Introduction. Because of our exclusion of mirrors, $M2$ does not appear here. $E1, E2, F$ are Fenyves' Extra Loop Axioms [3,4]:

$$E1: \ (x(yz))y = (xy)(zy) \qquad E2: \ (yz)(yx) = y((zy)x)$$
$$F: \ ((xy)z)x = x(y(zx))$$

Equation	Loop?	Reason	Name
$((xx)y)z = (xx)(yz)$	no	$I(2,1,3)$	42
$(x(xy))z = (xx)(yz)$	yes	3.1	$41, LCa$
$((xx)y)z = x(x(yz))$	no	$I(3,1,5)$	$48, LCb$
$(x(xy))z = x((xy)z)$	yes	$ASSOC$	47
$((xy)x)z = (xy)(xz)$	yes	$ASSOC$	11
$(x(yx))z = (xy)(xz)$	yes	3.1	12
$((xy)x)z = x(y(xz))$	yes	[6]	$17, N2$
$(x(yx))z = x((yx)z)$	yes	$ASSOC$	18
$((xy)z)x = (xy)(zx)$	yes	$ASSOC$	1
$(x(yz))x = (xy)(zx)$	yes	[6]	$2, M1$
$((xy)z)x = x(y(zx))$	yes	3.4	$6, F$
$(x(yz))x = x((yz)x)$	no	$FLEX$	9
$((xy)y)z = (xy)(yz)$	yes	$ASSOC$	31
$(x(yy))z = (xy)(yz)$	yes	3.2	32
$((xy)y)z = x(y(yz))$	no	$I(2,2,3)$	$37, C$
$(x(yy))z = x((yy)z)$	yes	3.1	38
$((xy)z)y = (xy)(zy)$	yes	$ASSOC$	21
$(x(yz))y = (xy)(zy)$	yes	3.3	$22, E1$
$((xy)z)y = x(y(zy))$	yes	[6]	$27, N1$
$(x(yz))y = x((yz)y)$	yes	$ASSOC$	28
$((xy)z)z = (xy)(zz)$	no	$RALT$	51
$(x(yz))z = (xy)(zz)$	no	$I(1,2,3)$	52
$((xy)z)z = x(y(zz))$	no	$I(1,3,5)$	$57, RCb$
$(x(yz))z = x((yz)z)$	yes	$ASSOC$	58

Table I

He shows that these are equivalent in *loops*. Since each of them implies that a quasigroup is a loop, they are also equivalent in quasigroups. Observe that $E2$ is the mirror of $E1$, while F is its own mirror. Fenyves lists three LC identities, and proves they are equivalent in loops, but in quasigroups we must list them separately, along with their mirrors, the RC identities:

$$\begin{array}{lll} LCa: & (x(xy))z = (xx)(yz) & \qquad RCa: \quad (zy)(xx) = z((yx)x) \\ LCb: & ((xx)y)z = x(x(yz)) & \qquad RCb: \quad ((zy)x)x = z(y(xx)) \\ LCc: & (x(xy))z = x(x(yz)) & \qquad RCc: \quad ((zy)x)x = z((yx)x) \end{array}$$

Note, from the table, that LCa implies that a quasigroup is a loop, whereas LCb does not; neither does LCc, which is of sub-form $T31R = T13R$, and thus does not appear in

the table at all. C denotes Fenyves' C-Loop axiom; this is its own mirror. He shows that in a loop, C implies all the LC and RC identities, but this is not true in quasigroups, since $I(2,2,3)$ satisfies C, but does not satisfy LCa or LCb.

Under "Reason", our table indicates the proof for the "yes" or "no" answer to "Loop?". The flag $ASSOC$ means that the law is easily seen to be equivalent to full associativity in a quasigroup. These are all of the form $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$, where α, β, γ are terms which can take on any triple of values. For the same reason, the two flagged as $FLEX$ and $RALT$ are easily seen to be equivalent to these two laws respectively, but by Lemma 2.3, that implies a "no" answer. For the rest of the "no" answers, we have simply listed a counter-example, which turns out to always be of the form $I(a,b,p)$ (see §2). The rest of the "yes" answers seem to require some proof, and we have listed, as a reference for the proof, either the paper [6] or a theorem number in this paper,

Fenyves points out that besides the equations we have flagged by $ASSOC$, it is easy to see that each of the equations 12, 32, and 52 is equivalent to full associativity in *loops*. As we see from the table, in *quasigroups*, this is still true for 12 and 32, but it is false for 52.

In this table, the four mirror pairs are: $\{48,57\}$, $\{47,58\}$, $\{17,27\}$, and $\{18,28\}$. The other equations of the form $T31 = T13$ are their own mirror, and the equations of form $T31 = T22$ have mirrors of the form $T13 = T22$, which we did not list.

We now proceed to prove the "yes" results stated in the table. First, we dispense with three of the equations for which the proof is easy:

3.1. Theorem. Each of the equations numbered 41, 12, 38 implies that a quasigroup is a loop.

Proof. For 41, $(x(xy))z = (xx)(yz)$: Fix a, b such that $ab = b$. Then for any x, $(x(xa))b = (xx)(ab) = (xx)b$. Cancelling, $xa = a$ for all x, so a is a right identity. Now, setting $z = a$ in 41 yields the law $LALT$, which implies a left identity by Lemma 2.2.

For 12, $(x(yx))z = (xy)(xz)$: Fix a, b such that $ab = b$. Then for any y, $(a(ya))b = (ay)(ab) = (ay)b$. Cancelling, $ya = y$, so a is a right identity. Setting $z = a$ in 12 yields $FLEX$, so apply Lemma 2.2.

For 38, $(x(yy))z = x((yy)z)$: Fix $d = (cc)$ for some c; so $(xd)z = x(dz)$ for all x, z. Now, fix a such that $ad = d$. Then $dz = a(dz)$ for all z. Since every element is of the form dz for some z, the element a is a left identity. By the mirror of this argument, there is also a right identity. □

Equation 38 simply states that all squares are in the middle nucleus, and our proof just shows that any quasigroup with a non-empty middle nucleus is a loop.

3.2. Theorem. The equation 32, $(x(yy))z = (xy)(yz)$, implies that a quasigroup is a loop.

Proof. Fix any e, b such that $eb = b$. Then for any x, $(x(ee))b = (xe)(eb) = (xe)b$. Cancelling, $ee = e$. Then, for any x, z, $(xe)z = (x(ee))z = (xe)(ez)$, so, by cancelling, $ez = z$, so e is a left identity.

Now, to show that e is a right identity, fix an element c, and we show $ce = c$. First, fix d such that $d(cc) = e$. Then $(d(cc))z = ez = z$ for any z, so equation 32 implies

$$(dc)(cz) = z \qquad (\alpha)$$

By (α), followed by (32) (with $x = dc$), $e(cc) = cc = ((dc)(cc))c = ((dc)c)(cc)$, so $e = (dc)c$. Since (α) implies $e = (dc)(ce)$ also, we cancel to get $ce = e$. □

The next two theorems use the method of proof of Lemma 2.7, utilizing the definitions $x \cdot j(x) = k(x) \cdot x = x$.

3.3. Theorem. The equation 22, $(x(yz))y = (xy)(zy)$, implies that a quasigroup is a loop.

Proof. First, we verify that $j(x) = k(x)$. To see this, fix a, and let $b = j(a)$, so $ab = a$. Then $(ba)a = (b(ab))a = (ba)(ba)$, so, cancelling yields $a = ba$, so $b = k(a)$. Now, we have $x \cdot j(x) = j(x) \cdot x = x$ for all x.

Next, we show that $j(x)$ is always an idempotent. To see this, apply equation 22:

$$j(x)\,x = x = (j(x)\,(j(x)\,x))\,j(x) = (j(x)\,j(x))\,(x\,j(x)) = (j(x)\,j(x))\,x$$

and cancel to get $j(x) = j(x)\,j(x)$.

Finally, we show that $j(x)$ is a constant, which must then be an identity element. To see this, fix c, d, and we show $j(c) = j(d)$. First, fix b such that $bd = j(c)$. Applying equation 22, we get

$$(x\,j(c))b = (xb)(db) \qquad (\beta)$$

Applying (β) with $x = c$ yields $cb = (cb)(db)$, and hence $db = j(cb)$. Thus, db is an idempotent, so applying (β) with $x = d$ yields $(d\,j(c))b = db$, so $d\,j(c) = d$, which implies that $j(c) = j(d)$. □

3.4. Theorem. The equation 6, $((xy)z)x = x(y(zx))$, implies that a quasigroup is a loop.

Proof. This equation is its own mirror, so that each time we prove a result, we also have the mirror of the result. First note that

$$\gamma 1:\ j(x)\,(j(x)\,x) = x \qquad\qquad \gamma 2:\ (x\,k(x))\,k(x) = x$$

To prove $(\gamma 1)$, use equation 6 to get $xx = ((x\,j(x))\,j(x))x = x(j(x)\,(j(x)\,x))$, and cancel. Next note that

$$\delta 1:\ j(x)\,j(x) = k(x) \qquad\qquad \delta 2:\ k(x)\,k(x) = j(x)$$

To prove $(\delta 1)$, apply $(\gamma 1)$ and equation 6 to get $((j(x)\,j(x))\,x)\,j(x) = j(x)\,(j(x)\,(x\,j(x))) = x = (k(x)\,x)\,j(x)$, and cancel.

Next, we show that $j(x) = k(x)$. To see this, fix a, and let $b = j(a)$ and $c = k(a)$, so $ab = ca = a$. Applying equation 6 (with $z = ac$ and $x = y = c$), along with $(\gamma 2)$ and $(\delta 2)$, we get

$$(b(ac))c = ((cc)(ac))c = c(c((ac)c)) = c(ca) = a = (ac)c$$

and we cancel to get $b(ac) = ac$. Thus, $k(ac) = b = j(a)$; squaring both sides and applying $(\delta 1)$ and $(\delta 2)$ yields $j(ac) = k(a) = c$. Thus, $ac = (ac) \cdot j(ac) = (ac)c = a$ (by $(\gamma 2)$), so $c = j(a) = b$.

We now have $j(x)j(x) = j(x)$ by $(\delta 1)$, and we proceed to prove the mirrors

$$\epsilon 1: \; j(x)\,(y\,j(x)) = y \qquad\qquad \epsilon 2: \; (j(x)\,y)\,j(x) = y$$

For $(\epsilon 2)$, use equation 6 and idempotency of $j(x)$ to get

$$(j(x)\,z)\,j(x) = ((j(x)\,j(x))\,z)\,j(x) = j(x) \cdot (j(x)\,(z\,j(x))) \qquad (*)$$

We also have the mirror equation, $j(x)\,(z\,j(x)) = ((j(x)\,z)\,j(x)) \cdot j(x)$. Putting these together, we have $j(x)\,(z\,j(x)) = \big(j(x) \cdot [j(x)\,(z\,j(x))]\big) \cdot j(x)$. Now, in a quasigroup, $\forall yx \exists z[j(x)\,(z\,j(x)) = y]$, so we have $y = (j(x)\,y)\,j(x)$.

Now, using $(\epsilon 1), (\epsilon 2)$ in $(*)$, we get $z = j(x) \cdot z$, so $j(z) = j(x)$, so $j(x)$ is a constant, which is then the identity element. □

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1958.

[2] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, 1990.

[3] F. Fenyves, Extra Loops I, *Publicationes Mathematicae Debrecen* 15 (1968) 235 – 238.

[4] F. Fenyves, Extra Loops II, *Publicationes Mathematicae Debrecen* 16 (1969) 187 – 192.

[5] J. Hart and K. Kunen, Single Axioms for Odd Exponent Groups, *J. Automated Reasoning* 14 (1995) 383 – 412.

[6] K. Kunen, Moufang Quasigroups, *J. Algebra*, to appear.

[7] W. W. McCune, OTTER 3.0 Reference Manual and Guide, Technical Report ANL-94/6, Argonne National Laboratory, 1994.

[8] W. W. McCune, A Davis-Putnam Program and its Application to Finite First-Order Model Search: Quasigroup Existence Problems, Technical Report, Argonne National Laboratory, 1995.

[9] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann Verlag, 1990.

[10] D. A. Robinson, Bol Quasigroups, *Publ. Math. Debrecen* 19 (1972) 151 – 153.

[11] J. Slaney, FINDER: Finite Domain Enumerator, Technical Report, Centre for Information Science Research, Australian National University, 1995.

Items [7] and [8] are available on WWW through `http://www.mcs.anl.gov/`
Items [5] and [6] are available on WWW through `http://math.wisc.edu:80/~kunen/`