MOUFANG MAGMAS WITH INVERSES

J. D. PHILLIPS

Abstract. There are four standard Moufang identities; call them $(M1), (M2), (M3)$, and $(M4)$ (their definitions are given below). In the variety of loops they are equivalent; that is, each of these identities implies the other three. It was shown in [8] that magmas with inverses that satisfy either $(M1)$ or $(M2)$ are, in fact, loops, while magmas with inverses that satisfy either $(M3)$ or $(M4)$ need not be loops. We show here that 2-divisible magmas with inverses that satisfy either $(M3)$ or $(M4)$ *are* loops. We also establish all implications between $(M1), (M2), (M3)$ and $(M4)$ in the variety of magmas with inverses.

A *groupoid* is a set with a single binary operation. A *quasigroup* $(Q, \cdot)$ is a groupoid such that for each $a, b \in Q$ the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions $x, y \in Q$. A *loop* is a quasigroup with a two-sided neutral element. For an overview of the theory of loops, see [1, 2, 5].

We write xy instead of $x \cdot y$, and stipulate that $\cdot$ have lower priority than juxtaposition, so for instance, $x \cdot yz$ stands for $x \cdot (y \cdot z)$.

Loop theory can also be expressed in the language of universal algebra: a *loop* is a set with three binary operations $\cdot$, $/$, $\backslash$ and a constant, 1, that satisfy the following six identities:

$$x \cdot (x\backslash y) = (y/x) \cdot x = x\backslash(x \cdot y) = (y \cdot x)/x = y$$

$$1 \cdot x = x \cdot 1 = x.$$

Thus, the class of loops is a variety of algebras of type $\langle 2, 2, 2, 0\rangle$.

Consider the following four groupoid identities:

$$(M1): \quad z(x \cdot zy) = (zx \cdot z)y \qquad (M2): \quad (xz \cdot y)z = x(z \cdot yz)$$

$$(M3): \quad (z \cdot xy)z = zx \cdot yz \qquad (M4): \quad z(xy \cdot z) = zx \cdot yz$$

In loops, each of $(M1), (M2), (M3)$, and $(M4)$ is equivalent to the other three [5]. In fact, the same is true in quasigroups, and in this case, they are loops [3]. These identities are the four standard *Moufang* laws. Clearly, the class of Moufang loops can be realized as a variety of algebras of type $\langle 2, 2, 2, 0\rangle$.

1991 *Mathematics Subject Classification.* Primary: 20N05. Secondary: 03C05.
Key words and phrases. magma with inverses, loop, group, Moufang.

A *magma* is a groupoid with a two-sided neutral element[1]. We say that a magma M is *with inverses* if for every $x \in M$ there is a $y \in M$ satisfying $xy = yx = 1$. We then call y an *inverse* of x, noting that x can have several inverses. *Groups* are thus associative magmas with inverses. Viewed this way, then, groups are algebras of type $\langle 2, 1, 0\rangle$. This is a "cleaner" and more familiar axiomatization than is the rather awkward axiomatization of Moufang loops as algebras of type $\langle 2, 2, 2, 0\rangle$. And so the obvious question is: *Can the variety of Moufang loops be realized as algebras of type* $\langle 2, 1, 0\rangle$; i.e., as magmas with inverses that satisfy one of the Moufang laws?

Somewhat surprisingly, the answer depends on which of the four Moufang laws one uses in the axiomatization. To wit, in [8] it is shown that magmas with inverses that satisfy either $(M1)$ or $(M2)$ are loops, while magmas with inverses that satisfy either $(M3)$ or $(M4)$ need not be loops. Here, we concern ourselves with the obvious, and harder, question: *How close are magmas with inverses that satisfy either* $(M3)$ *or* $(M4)$ *to being loops?*

In preparation for the next four lemmas, we offer the following definitions: A magma is *flexible* if it satisfies $xy \cdot x = x \cdot yx$, and it is *left alternative* if it satisfies $x \cdot xy = xx \cdot y$.

Now, let L be a magma with inverses. As noted above, inverses need not be unique, thus, x^{-1} is not well-defined. So, in the next three definitions, x^{-1} represents any inverse of x (that is, the identities must hold for each and every inverse of x). L has the *left inverse property* if $x^{-1} \cdot xy = y$, the *right inverse property* if $yx \cdot x^{-1}$, and the *antiautomorphic inverse property* if $(xy)^{-1} = y^{-1}x^{-1}$.

Lemma 1. *Let L be a magma with inverses that satisfies* $(M1)$. *Then, L is flexible and left alternative; moreover, L has the left inverse property, the right inverse property, and the antiautomorphic inverse property.*

Proof. Setting $y = 1$ in $(M1)$ gives flexibility. Setting $x = 1$ in $(M1)$ gives left alternativity.

Next, it's easy to see that $x((xx)^{-1} \cdot x) = (x \cdot (xx)^{-1})x = 1$. Thus,

[1] The definitions of *groupoid* and *magma* are often interchanged in the literature.

$$\begin{aligned} x^{-1} \cdot xy &= 1 \cdot (x^{-1} \cdot xy) \\ &= (x(xx)^{-1} \cdot x) \cdot (x^{-1} \cdot xy) \\ &= x((xx)^{-1} \cdot (x(x^{-1} \cdot xy))) \\ &= x((xx)^{-1} \cdot ((xx^{-1} \cdot x)y)) \\ &= x((xx)^{-1} \cdot xy) \\ &= (x(xx)^{-1} \cdot x) \cdot y \\ &= 1 \cdot y \\ &= y. \end{aligned}$$

The right inverse property is proved similarly. Finally, $y^{-1}x^{-1} = ((xy)^{-1} \cdot (xy \cdot y^{-1}))x^{-1} = ((xy)^{-1} \cdot x)x^{-1} = (xy)^{-1}$.

□

Lemma 2. *If a magma with inverses satisfies* $(M1)$ *then it satisfies* $(M3)$.

Proof. It is easy to show that $(x^{-1})^{-1} = x$, $x \cdot x^{-1}y = y$, and $yx^{-1} \cdot x = y$.

Next, we have

$$\begin{aligned} (x \cdot yz) \cdot (z^{-1}x) &= (x \cdot (y(x \cdot x^{-1}z))) \cdot (x^{-1}z)^{-1} \\ &= ((xy \cdot x)(x^{-1}z)) \cdot (x^{-1}z)^{-1} \\ &= xy \cdot x \\ &= x \cdot yx. \end{aligned}$$

Now, use this to obtain

$$\begin{aligned} x(yz \cdot x) &= x((yz \cdot z^{-1})z \cdot x) \\ &= x((yz \cdot z^{-1})z \cdot z^{-1}) \cdot ((z^{-1})^{-1}x) \\ &= xy \cdot zx. \end{aligned}$$

□

Lemma 3. *A magma with inverses satisfies* $(M1)$ *if and only if it satisfies* $(M2)$.

Proof. We have

$$\begin{aligned} (xy \cdot z)y &= (xy \cdot z)(x^{-1} \cdot xy) \\ &= (xy \cdot zx^{-1})(xy) \\ &= (((xy \cdot zx^{-1})(xy)) \cdot y^{-1})(y^{-1})^{-1} \\ &= ((xy) \cdot ((zx)^{-1}(xy \cdot y^{-1}))) \cdot (y^{-1})^{-1} \\ &= ((xy)(zx^{-1} \cdot x)) \cdot y \\ &= ((x(y \cdot zx^{-1})) \cdot x)y \\ &= x((y \cdot zx^{-1})(xy)) \\ &= x(y((zx^{-1} \cdot x)y)) \\ &= x(y \cdot zy). \end{aligned}$$

The proof of the converse is similar. □

Lemma 4. *A magma satisfies* $(M3)$ *if and only if it satisfies* $(M4)$*.*

Proof. Setting $x = 1$ in $(M3)$ gives flexibility, and $(M4)$ follows. The proof of the converse is similar. □

We may thus focus our investigations on either $(M3)$ or $(M4)$. We investigate $(M3)$.

We note the following easy fact: *given* $n > 2$*, there is a magma with inverses of size* n *that satisfies* $(M3)$ *but that is not a loop.* To see this, define a binary operation, $\cdot$, on $\{1, 2, \ldots, n\}$ as follows: if neither x nor y is 1, set $x \cdot y = 1$; otherwise, set $x \cdot 1 = 1 \cdot x = x$. Clearly, this is a magma with inverses, and if $n > 2$, it is not a loop. Finally, an easy check shows that it satisfies $(M3)$. Note that in this example inverses are not unique. In the next example inverses are unique.

Example 5. A magma with unique inverses that satisfies $(M3)$ but is not a loop.

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

These examples—of every size $n > 2$—seem to suggest that magmas with inverses that satisfy $(M3)$ are very far from being loops. The next theorem shows that they are closer than you might think. First, we need a preparatory definition: a groupoid is *2-divisible* if each of its elements can be written as a square, in other words, if each element has a (not necessarily unique) square root.

Theorem 6. *If* L *is a 2-divisible magma with inverses that satisfies* $(M3)$*, then* L *is a loop.*

Proof. Automated theorem provers are now a common tool in loop theory [7]. We used Prover9 [4] to prove Theorem 6. The proof we generated with this powerful tool is complicated in at least two ways. Firstly, Prover9 was unable to find a proof of this theorem directly; that is, we had to employ the rather sophisticated "proof sketches" strategy [9]. And secondly, the proof we ultimately generated is long and complicated. Even after employing some "proof shortening" techniques, the shortest proof we were able to generate is over 250 lines long. You may find a copy of this proof at:

`http://euclid.nmu.edu/~jophilli/moufang-magma.html`

This proof is too complicated to easily translate into a "human friendly" form. But this is no cause for alarm since (1) it is easy to write a very short program (in, e.g., C or java or python) to verify the proof and (2) it is becoming increasingly common in loop theory to publish results obtained via automated theorem provers *sans* translated proofs, but instead with links to the proof's dense output file [6].

□

References

[1] В. Д. Белоусов, *Основы Теории Квазигрупп и Луп*, Издательство «Наука», Москва, 1967.

[2] R. H. Bruck, *A Survey of Binary Systems*, Springer, 1971.

[3] K. Kunen, Moufang quasigroups *Journal of Algebra*, **183** (1996) no. 1, 231–234.

[4] W. W. McCune, `Prover9` and `Mace`, download at http://www.prover9.org

[5] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann, 1990.

[6] J. D. Phillips and D. Stanovský, Bruck loops with abelian inner mapping groups, *Communications in Algebra*, to appear.

[7] J. D. Phillips and D. Stanovský, Automated theorem proving in quasigroup and loop theory, *AI Communications*, **23** (2010), no. 2–3, 267–283.

[8] J. D. Phillips and P. Vojtěchovský, A scoop from groups: new equational foundations for loops, *Commentationes Mathematicae Universitatis Carolinae*, **49**, (2008), no. 2, 279–290.

[9] R. Veroff, Solving open questions and other challenge problems using proof sketches. *J. Automated Reasoning*, 27(2):157–174, 2001.

Department of Mathematics & Computer Science, Northern Michigan University, Marquette, MI 49855 USA

E-mail address: `jophilli@nmu.edu`

URL: `http://euclid.nmu.edu/~jophilli/`