A Generalization of Moufang and Steiner Loops

Kinyon, M., Kunen, K., & Phillips, J.

A GENERALIZATION OF MOUFANG AND STEINER LOOPS

MICHAEL K. KINYON, KENNETH KUNEN*, AND J.D. PHILLIPS

Abstract. We study a variety of loops, RIF, which arise naturally from considering inner mapping groups, and a somewhat larger variety, ARIF. All Steiner and Moufang loops are RIF, and all flexible C-loops are ARIF. All ARIF loops are diassociative.

1. Introduction

A *loop* is an algebraic system $(L;\ \cdot, \backslash, /, 1)$ satisfying the equations

$$x \cdot (x\backslash y) = x\backslash(x \cdot y) = (y/x) \cdot x = (y \cdot x)/x = y \cdot 1 = 1 \cdot y = y \quad .$$

See the books [1, 4, 13] for further information. Since loops in general form too broad a class for detailed study, the literature has focused on various sub-varieties of loops.

Many of these varieties are defined by some weakening of the *associative* law, $x \cdot yz = xy \cdot z$. Some obvious weakenings are the *flexible* laws and the *left* and *right alternative* laws:

$$\text{FLEX} : x \cdot yx = xy \cdot x \quad \text{RALT} : x \cdot yy = xy \cdot y \quad \text{LALT} : y \cdot yx = yy \cdot x.$$

There is also the *inverse property, IP*. This asserts that there is a permutation J of order two such that (writing x^{-1} for xJ) left and right division are given by $x\backslash y = x^{-1}y$ and $y/x = yx^{-1}$. To see that the IP defines a variety of loops, note that it can be expressed by the equations $x\backslash y = (x/1)\, y$ and $y/x = y\,(1/x)$. Most of the loops considered in this paper have the IP. The IP implies the antiautomorphic inverse property (AAIP), $(xy)^{-1} = y^{-1}x^{-1}$, so that J provides an isomorphism from the loop $(L;\cdot)$ onto its opposite loop $(L;\circ)$ (where $x \circ y = y \cdot x$). Thus, in IP loops, the right and left versions of properties (e.g., RALT and LALT) are equivalent.

In a loop L, the left and right translations by $x \in L$ are defined by $yL(x) = xy$ and $yR(x) = yx$, respectively. The *multiplication group* of L is the permutation group on L, $\mathrm{Mlt}(L) = \langle R(x), L(x) : x \in L\rangle$, generated by all left and right translations. The *inner mapping group* is the subgroup $\mathrm{Mlt}_1(L)$

Date: May 28, 2018.

1991 *Mathematics Subject Classification.* Primary 20N05.

Key words and phrases. Moufang loop, Steiner loop, RIF, ARIF, diassociative.

*Author supported by NSF Grant DMS-9704520.

This paper is in final form, and no version of it will be submitted for publication elsewhere.

fixing 1. If L is a group, then $\mathrm{Mlt}_1(L)$ is the group of inner automorphisms of L. In an IP loop, the AAIP implies that we can conjugate by J to get:

$$L(x)^J = R(x^{-1}) \quad R(x)^J = L(x^{-1})$$

where $\theta^J = J^{-1}\theta J = J\theta J$ for a permutation θ. If θ is an inner mapping, then so is θ^J. This leads us to one of the classes of IP loops we study in this paper:

Definition 1.1. *A* RIF loop *is an IP loop L with the property that $\theta^J = \theta$ for all $\theta \in \mathrm{Mlt}_1(L)$. Equivalently, inner mappings preserve inverses, i.e., $(x^{-1})\theta = (x\theta)^{-1}$ for all $\theta \in \mathrm{Mlt}_1(L)$ and all $x \in L$.*

RIF loops include the *Steiner loops*, which may be defined to be IP loops of exponent two (that is, $x^{-1} = x$, so J is the identity permutation). Steiner loops arise naturally in combinatorics, since they correspond uniquely to Steiner triple systems; specifically, the Steiner loop L corresponds to the triple system $\{\{x, y, xy\} : x \neq y \ \&\ x, y \neq 1\}$ on $L \setminus \{1\}$.

RIF loops also include what is probably the most well-studied class of nonassociative loops, namely those satisfying the *Moufang laws* [11, 12]:

Definition 1.2. *A* Moufang loop *is a loop satisfying the following equations:*

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

In fact, by work of Bol and Bruck, each of these equations implies the other three (see Bruck [1], Lemma 3.1, p. 115). That every Moufang loop is RIF follows from Lemma 3.2, p. 117, of [1]. It is easily seen that the only loops which are both Steiner and Moufang are the boolean groups. Thus a direct product of a nonassociative Steiner loop with a nonassociative Moufang loop is a RIF loop which is neither Steiner nor Moufang.

A loop is said to be *diassociative* if the subloop $\langle x, y\rangle$ generated by any two elements is a group. Diassociative loops are always IP loops, and are flexible and alternative. Steiner loops are obviously diassociative; in fact each $\langle x, y\rangle$ is a boolean group (of order 1, 2, or 4). Less obviously, by Moufang's Theorem, every Moufang loop is diassociative.

Bruck and Paige [2] defined an *A-loop* to be a loop in which every inner mapping is an automorphism. An A-loop need not be an IP-loop, but they show, by modifying the proof of Moufang's Theorem, that every IP A-loop is diassociative. In fact, it turned out later [8] that the IP A-loops form a proper sub-variety of the Moufang loops. Weakening of the notion of IP A-loop so that inner mappings preserve inverses, but not necessarily products, we obtain RIF loops.

The notion "RIF" can be expressed by a finite set of equations (Lemma 2.2). These lead naturally (Lemma 2.4) to a slightly weaker notion, ARIF.

Definition 1.3. *An ARIF loop is a flexible loop satisfying the following equations:*

$$W1 : R(x)R(yxy) = R(xyx)R(y) \qquad W2 : L(x)L(yxy) = L(xyx)L(y)$$

In fact, a flexible loop satisfying either W1 or W2 has the IP and hence satisfies both equations (Lemma 2.7). Every ARIF loop of odd order is Moufang (Corollary 2.14) (whereas non-group Steiner loops are RIF and not Moufang). Besides RIF loops, ARIF includes another variety of IP loops, namely the flexible C-loops (Corollary 2.6). C-loops were introduced by Fenyves [6]; see Section 2. There exist flexible C-loops which are not RIF loops (Example 4.1), and there exist ARIF loops which are neither RIF loops nor C-loops (see Section 4).

Acronym 1.4. *A = Almost, R = Respects, I = Inverses, F = Flexible.*

Section 3 is devoted to the proof of our main result, a generalization of Moufang's Theorem to ARIF loops:

Theorem 1.5. *Every ARIF loop is diassociative.*

Our inductive proof of this theorem is patterned on Moufang's proof, but is quite a bit more complicated than hers, or than the corresponding proof in Bruck and Paige [2] for IP A-loops. We do not know a simpler proof, but Example 4.3 shows that the basic lemma on associators developed by Moufang can fail in a ARIF loop (in fact, in a Steiner loop).

Note that if we write out the definition of diassociativity in the obvious way, we get an infinite list of equations. The following problem, asked first by Evans and Neumann [5], is still open:

Question 1.6. *Does the variety of diassociative loops have a finite basis?*

If the answer is "yes", which seems unlikely, then inductive proofs of diassociativity could always be replaced by the verification of a finite number of instances of diassociativity, which could result in a simplification.

Our investigations were aided by the automated reasoning tools OTTER, developed by McCune [10], and SEM developed by J. Zhang and H. Zhang [14]. SEM finds finite models of systems of axioms, and was used to produce the three examples in Section 4. OTTER derives statements from axioms, and was used to derive enough instances of diassociativity from ARIF for the pattern to become clear.

2. Basics

Following Bruck [1] (see IV.1), the inner mapping group of any loop is generated by the inner mappings of the form $L(x, y)$, $R(x, y)$, and $T(x)$:

Definition 2.1. $T(x) = R(x)L(x)^{-1}$
$L(x, y) = L(x)L(y)L(yx)^{-1} \qquad R(x, y) = R(x)R(y)R(xy)^{-1}$

Using this, we can express the notion of RIF by equations.

Lemma 2.2. *The following are equivalent for an IP loop L:*

1. *L is a RIF loop.*
2. *L is flexible and $R(x,y) = L(x^{-1}, y^{-1})$ for all $x, y \in L$.*
3. *$R(xy)L(xy) = L(y)L(x)R(x)R(y)$ for all $x, y \in L$.*
4. *$L(xy)R(xy) = R(x)R(y)L(y)L(x)$ for all $x, y \in L$.*

Proof. The flexible law can be expressed as $R(x)L(x) = L(x)R(x)$ for all x. In an IP loop, this is equivalent to $L(x^{-1})R(x) = R(x)L(x^{-1})$, that is, $T(x)^J = T(x)$. Also, an easy calculation gives $R(x,y)^J = L(x^{-1}, y^{-1})$ in an IP loop. Thus (1) and (2) are equivalent. Using the IP and Definition 2.1, $R(x,y) = L(x^{-1}, y^{-1})$ is equivalent to $L(xy)R(xy) = L(y)L(x)R(x)R(y)$. Since the flexible law is just $R(z)L(z) = L(z)R(z)$, (2) implies (3). Conversely, if (3) holds, then taking $y = 1$ gives the flexible law, so that (3) implies (2). Finally, (3) and (4) are equivalent by the IP. □

Combining 3 and 4 from Lemma 2.2 we obtain the very useful identity $L(y)L(x)R(x)R(y) = R(x)R(y)L(y)L(x)$, which we will frequently appeal to in our arguments.

For the next result, we introduce the notation $P(x) = L(x)R(x)$.

Corollary 2.3. *In a RIF loop, $P(xyx) = P(x)P(y)P(x)$.*

Proof. Applying Lemma 2.2 twice, $P(x \cdot yx) = R(x)R(yx)L(yx)L(x) = R(x)\ L(x)L(y)R(y)R(x)\ L(x) = P(x)P(y)P(x)$. □

The fact that Moufang loops satisfy $P(xyx) = P(x)P(y)P(x)$ is Theorem 5.1, p. 120, of Bruck [1]. The same theorem points out that $L(xyx) = L(x)L(y)L(x)$ and $R(xyx) = R(x)R(y)R(x)$ also hold in Moufang loops. But in flexible loops, these are simply restatements of the Moufang equations $N1, N2$ in Definition 1.2, so they do not hold in all RIF loops, since they fail in any non-group Steiner loop.

Next we show that RIF loops satisfy equations W1, W2 of Definition 1.3.

Lemma 2.4. *Every RIF loop is an ARIF loop.*

Proof. Equations W1, W2 are equivalent in IP loops. To prove W1, start with $R(v)R(y)L(y)L(v) = L(y)L(v)R(v)R(y)$, which is

$$v(y(zv)y) = (v(yz)v)y \quad ,$$

and set $v = ux$ and $z = u^{-1}$, so that $zv = x$. We get

$$ux \cdot yxy = (ux \cdot yu^{-1} \cdot ux)y \quad .$$

But $R(u^{-1})R(ux)L(ux) = R(x)L(x)L(u)$ (see Lemma 2.2), so

$$ux \cdot yxy = (u \cdot xyx)y \quad ,$$

which is W1. □

Next we show that every flexible C-loop is an ARIF loop. *C-loops*, introduced by Fenyves [6], are loops satisfying the equation $((xy)y)z = x(y(yz))$. These have the IP (see [6], Theorem 4) and are alternative (see [6], Theorem

3). They are not necessarily flexible (see Example 4.2). Every Steiner loop is trivially a C-loop; in fact, Table 1 of [6], a C-loop which is not Moufang, is just the 10-element Steiner loop.

Theorem 2.5. *Every C-loop satisfies*

$$R(xy)^2 = R(x)R(y(xy)) = R((xy)x)R(y).$$

Proof. Since the loop is alternative, the C-loop property can be written as $R(a)^2R(b) = R(a^2b)$. This gives us:

$$R(xy)^2R(y^{-1}) = R((xy)^2y^{-1}) = R((xy)((xy)y^{-1})) = R((xy)x) \quad .$$

so $R(xy)^2 = R((xy)x)R(y)$. Now, if $x = v^{-1}$ and $y = v(uv)$, we have $xy = uv$ and hence $R(uv)^2 = R(u)R(v(uv))$. □

Corollary 2.6. *Every flexible C-loop is a ARIF loop.*

We now examine basic properties of ARIF loops.

Lemma 2.7. *A loop satisfying*

$$W1': \qquad R(x)R((yx)y) = R(x(yx))R(y)$$

is an alternative IP loop.

Proof. Let x^{-1} denote $1/x$, so that $x^{-1}x = 1$. Applying W1′ to x^{-1} gives $(yx)y = (x^{-1}(x(yx)))y$, and cancelling gives $yx = x^{-1}(x(yx))$. Replacing y with $(x\backslash y)/x$ yields $x\backslash y = x^{-1}y$. In particular $1 = x(x^{-1}1) = xx^{-1}$, and so $(x^{-1})^{-1} = x$. Next apply W1′ to $(x(yx))^{-1}$ to get $((x(yx))^{-1}x)((yx)y) = y$, and thus $(yx)y = ((x(yx))^{-1}x)^{-1}y$. Cancelling yields $yx = ((x(yx))^{-1}x)^{-1}$. Replacing y with y/x gives $y = ((xy)^{-1}x)^{-1}$ and so $y^{-1} = (xy)^{-1}x$, which implies $(xy)y^{-1} = x$. Replacing x with x/y gives $xy^{-1} = x/y$. Thus the loop satisfies the IP. Setting $y = 1$ in W1′ yields the right alternative law $R(x)R(x) = R(xx)$, and the right and left alternative laws are equivalent in IP loops. □

Corollary 2.8. *Every ARIF loop is an alternative IP loop.*

Lemma 2.9. *Every ARIF loop satisfies* $R(x)R(y^2x^{-1})R(x) = R(xy^2)$ *and* $L(x)L(x^{-1}y^2)L(x) = L(y^2x)$.

Proof. The second equation is equivalent to the first in IP loops. So start with $R(aba)R(b) = R(a)R(bab)$.
Set $b = xy$ and $a = x^{-1}$ (so $ab = y$) to get

$$R(yx^{-1})R(xy) = R(x^{-1})R(xy^2).$$

Set $b = x$ and $a = yx^{-1}$ (so $ab = y$) to get

$$R(y^2x^{-1})R(x) = R(yx^{-1})R(xy).$$

Putting these together, we have

$$R(y^2x^{-1})R(x) = R(x^{-1})R(xy^2).$$

□

Corollary 2.10. *Every ARIF loop in which each element is a square is a Moufang loop.*

Proof. Now we have $R(x)R(yx^{-1})R(x) = R(xy)$. If we let $z = yx^{-1}$ and $y = zx$, we get $R(x)R(z)R(x) = R(xzx)$, which (in flexible loops) is the Moufang equation N1 of Definition 1.2. □

In general, products of an element of a loop with itself do not associate, e.g., $x \cdot xx \neq xx \cdot x$. We shall see that this problem does not arise in ARIF loops. Until then, we let x^n denote the right-associated product.

Definition 2.11. *Define* $x^n = (1)(L(x))^n$ *for any* $n \in \mathbb{Z}$.

Thus, $x^3 = x \cdot xx$, and (in an IP loop) $x^{-3} = (1)L(x^{-1})^3 = x^{-1} \cdot x^{-1}x^{-1}$, whereas $(x^3)^{-1} = x^{-1}x^{-1} \cdot x^{-1}$.

Definition 2.12. *A loop* L *is* power associative *iff for all* $x \in L$*, the subloop* $\langle x \rangle$ *generated by* x *is a group, and* power alternative *iff* $L(x^i) = (L(x))^i$ *and* $R(x^i) = (R(x))^i$ *for all* $x \in L$ *and all* $i \in \mathbb{Z}$

It is easily seen that diasociativity implies power alternativity and power alternativity implies power associativity.

Now for $n > 0$, let us say that an IP loop L is *n–PA* iff $L(x^m) = (L(x))^m$ whenever $1 \leq m \leq n$ and $x \in L$. So, the 1–PA is trivial and the 2–PA (that is, $xx \cdot y = x \cdot xy$) is equivalent to the alternative law. Hence, a 2–PA loop satisfies $x^3 = xx \cdot x = x \cdot xx$ and $x^{-3} = (x^3)^{-1}$. An IP loop which is n–PA for all $n > 0$ is power alternative. Note that the n–PA implies that $x^i \cdot x^j = (1L(x)^j)L(x)^i = x^{i+j}$ whenever $1 \leq i, j \leq n$. For $0 < j < k$, set $m = jk$, and suppose that L is k–PA. Then $x^m = 1(L(x)^j)^k = (1)L(x^j)^k = (x^j)^k$ by the j–PA, so $L(x^m) = L(x^j)^k = L(x)^m$ by the k–PA and j–PA. Thus L is m–PA, so the smallest n such that the n–PA fails must be prime.

Theorem 2.13. *Every ARIF loop is power alternative.*

Proof. By Corollary 2.8 and the preceding remarks, it is sufficient to prove that the ARIF loop L is n–PA for all odd $n \geq 3$. So, for $n = 2k + 1$, $k \geq 1$, assume that L is $2k$–PA. Setting $y = x^k$ in Lemma 2.9, we get $L(x)L(x^{-1}(x^k)^2)L(x) = L((x^k)^2)x)$. Now $(x^k)^2 = x^{2k}$ and $x^{-1}x^{2k} = x^{-1}(xx^{2k-1}) = x^{2k-1}$, and so, by the $(2k-1)$–PA, we have $L(x)^{2k+1} = L(x^{2k}x)$. Applying this to 1 gives $x^{2k+1} = x^{2k}x$, so $L(x)^n = L(x^n)$, which is the n–PA. □

Corollary 2.14. *Every finite ARIF loop of odd order is Moufang.*

Proof. In a power alternative loop L, the subloop $\langle x \rangle$ generated by a given $x \in L$ induces a coset decomposition of L, and so if L is finite, the order of x must divide the order of L. Thus in a power alternative loop of odd order, each element is a square. Now apply Corollary 2.10. □

3. Diassociativity

Moufang loops are diassociative by Moufang's Theorem. The same holds for ARIF loops (Theorem 1.5), as we show in this section. First, a lemma which generalizes Lemma 2.9:

Lemma 3.1. *In any ARIF loop:*

1. $R(yx^m)R(x^ny^{-1}) = R(yx^{m+k})R(x^{n-k}y^{-1})$
2. $R(x^my)R(y^{-1}x^n) = R(x^{m+k}y)R(y^{-1}x^{n-k})$
3. $L(x^my)L(y^{-1}x^n) = L(x^{m+k}y)L(y^{-1}x^{n-k})$
4. $L(yx^m)L(x^ny^{-1}) = L(yx^{m+k})L(x^{n-k}y^{-1})$

whenever $m, n, k \in \mathbb{Z}$ and either k is even or $m+n$ is even.

Proof. We focus on (1,2), since (3,4) are equivalent by the IP. Let L be a ARIF loop. On $\mathbb{Z}^2$, define three relations by

$$\begin{aligned}
(m,n) \sim_1 (s,t) &\iff \forall x,y \in L\,[R(yx^m)R(x^{-n}y^{-1}) = R(yx^s)R(x^{-t}y^{-1})]\\
(m,n) \sim_2 (s,t) &\iff \forall x,y \in L\,[R(x^{-m}y)R(y^{-1}x^n) = R(x^{-s}y)R(y^{-1}x^t)]\\
(m,n) \sim (s,t) &\iff (m,n) \sim_1 (s,t) \text{ and } (m,n) \sim_2 (s,t)\ .
\end{aligned}$$

Now $(m,n) \sim_1 (s,t) \longleftrightarrow (m,s) \sim_2 (n,t)$, and so

$$(m,n) \sim (s,t) \longleftrightarrow (m,s) \sim (n,t)\ . \tag{A}$$

It is clear that each of $\sim_1, \sim_2, \sim$ is an equivalence relation. By (A) and the fact that $\sim$ is symmetric:

$$(m,n) \sim (s,t) \longleftrightarrow (n,m) \sim (t,s)\ . \tag{B}$$

Also, replacing x by x^{-1} we have

$$(m,n) \sim (s,t) \longleftrightarrow (-m,-n) \sim (-s,-t)\ . \tag{C}$$

Replacing y by yx^j we have

$$(m,n) \sim (s,t) \longleftrightarrow (m+j,n+j) \sim (s+j,t+j)\ . \tag{D}$$

So far, everything we have said holds in any IP power alternative loop. Our goal is now to prove $(m,n) \sim (m+k,n+k)$ whenever $m,n,k \in \mathbb{Z}$ and either k is even or $m+n$ is even.

In the equations

$$R(yxy)R(x) = R(y)R(xyx)\ \ ;\ \ R(xyx)R(y) = R(x)R(yxy)\ \ ,$$

set $x = a^\alpha b^{-1}$ and $y = ba^\delta$. Then, by power alternativity,

$$xy = a^{\alpha+\delta}a^{-\delta}b^{-1}\cdot ba^\delta = a^{\alpha+\delta}(ba^\delta)^{-1}\cdot ba^\delta = a^{\alpha+\delta}\ \ ,$$

so that $xyx = a^{2\alpha+\delta}b^{-1}$ and $yxy = ba^{\alpha+2\delta}$. We get:

$$\begin{aligned}
R(ba^{\alpha+2\delta})R(a^\alpha b^{-1}) &= R(ba^\delta)R(a^{2\alpha+\delta}b^{-1})\\
R(a^{2\alpha+\delta}b^{-1})R(ba^\delta) &= R(a^\alpha b^{-1})R(ba^{\alpha+2\delta})\ .
\end{aligned}$$

The first of these equations implies $(\alpha+2\delta,-\alpha) \sim_1 (\delta,-2\alpha-\delta)$, while the second implies $(-2\alpha-\delta,\delta) \sim_2 (-\alpha,\alpha+2\delta)$, so (B) yields $(\alpha+2\delta,-\alpha) \sim$

$(\delta, -2\alpha - \delta)$. Set $\alpha = -m - 2c$ and $\delta = m + c$ to get $(m, m + 2c) \sim (m + c, m + 3c)$. Iterating this:

$$(m, m + 2c) \sim (m + jc, m + (j + 2)c) \tag{E}$$

for every $m, c, j \in \mathbb{Z}$. But by (A), we also have $(m, m+c) \sim (m+2c, m+3c)$, and iterating this we get:

$$(m, m + c) \sim (m + 2jc, m + (2j + 1)c) \tag{F}$$

for every $m, c, j \in \mathbb{Z}$.

Now, in view of (D), the lemma is equivalent to:

$$n \text{ even or } k \text{ even } \longrightarrow (0, n) \sim (k, n + k) \quad . \tag{$*$}$$

We prove by induction on n that $(*)$ holds for all k. By (C), it is sufficient to consider $n \geq 0$, and the $n = 0$ case holds by the IP. Now, fix $n > 0$.

If n is even, we need to prove $(0, n) \sim (k, n + k)$ for all k. Setting $c = \frac{n}{2}, m = k$ in (E) we get $(k, n+k) \sim (k+j\frac{n}{2}, n+k+j\frac{n}{2})$, so it is sufficient to prove $(0, n) \sim (k, n + k)$ whenever $0 \leq k < \frac{n}{2}$. But since this is the same as $(0, k) \sim (n, n + k)$, it follows by applying $(*)$ inductively to k, since n is even.

If n is odd, we need to prove $(0, n) \sim (2k, n + 2k)$ for all k. Setting $c = n, m = 2k$ in (F) we get $(2k, n + 2k) \sim (2k + 2jn, n + 2k + 2jn)$, so it is sufficient to prove $(0, n) \sim (2k, n + 2k)$ whenever $0 \leq 2k < 2n$. Now n is odd, so $2k \neq n$. If $0 \leq 2k < n$, then $(0, n) \sim (2k, n + 2k)$ (equivalently, $(0, 2k) \sim (n, n+2k)$) follows by applying $(*)$ inductively to $2k$. If $n < 2k < 2n$, then induction gives us instead $(0, 2n - 2k) \sim (-n, n - 2k)$, and hence (by (A,C)) $(0, n) \sim (2k-2n, 2k-n)$. But also $(0, n) \sim (-2n, -n)$ (by (F) with $c = n, m = 0, j = -1$), so $(2k, n + 2k) \sim (2k - 2n, 2k - n)$ (by (D)), and hence $(2k, n + 2k) \sim (0, n)$. □

We remark that one cannot remove the restriction on m, n, k. For example, if $R(yx)R(y^{-1}) = R(y)R(xy^{-1})$ (that is $(1, 0) \sim (0, -1)$) holds, then the loop must be Moufang (see the proof of Corollary 2.10). Conversely, Moufang loops satisfy the lemma for all m, n, k. To see this, note that we now have $(m+1, m) \sim (m, m-1)$ for every m, and hence $(m+1, m) \sim (n+1, n)$ for every m, n. So, $(m, n) \sim (m + 1, n + 1)$ for every m, n, and hence $(m, n) \sim (m + k, n + k)$ for every m, n, k.

The following lemma will be useful in the proof of diassociativity:

Lemma 3.2. *In a ARIF loop, suppose that p, a, q satisfy:*

$$p \cdot aq = pa \cdot q$$
$$pa \cdot a^{-1}q = pa^{-1} \cdot aq = pq \quad .$$

Then $pa^m \cdot a^n q = pa^{m+k} \cdot a^{n-k}q$ for all m, n, k.

Proof. We first verify

$$p \cdot a^{-1}q = pa^{-1} \cdot q \quad :$$

Applying Definition 1.3 twice, $R(x)R(y)R(xyx) = R(xyx)R(y)R(x)$. Let $x = q$ and $y = q^{-1}a^{-1}$, so $xyx = a^{-1}q$. Let $z = pa$. Then

$$zR(x)R(y) = (pa \cdot q)(q^{-1}a^{-1}) = (p \cdot aq)(q^{-1}a^{-1}) = p \quad ,$$

so $zR(x)R(y)R(xyx) = p \cdot a^{-1}q$. Also, $zR(xyx) = pa \cdot a^{-1}q = pq$, so

$$zR(xyx)R(y) = pq \cdot q^{-1}a^{-1} = (pa^{-1} \cdot aq) \cdot q^{-1}a^{-1} = pa^{-1} \quad ,$$

so $zR(xyx)R(y)R(x) = pa^{-1} \cdot q$.

Apply $R(q^{-1}a^{-1})R(a^{s+1}q) = R(q^{-1}a^0)R(a^sq)$ to $pa^0 \cdot a^1q = pa^1 \cdot a^0q$ to get $pa^0 \cdot a^{s+1}q = pa^1 \cdot a^sq$ whenever s is even. Then apply $L(a^0p^{-1})L(pa^t) = L(a^{-1}p^{-1})L(pa^{t+1})$ to get $pa^t \cdot a^{s+1}q = pa^{t+1} \cdot a^sq$ whenever s, t are even. Now, the same argument starting from $pa^0 \cdot a^{-1}q = pa^{-1} \cdot a^0q$ results in $pa^t \cdot a^{s+1}q = pa^{t-1} \cdot a^{s+2}q$ whenever s, t are even. Applying these with $(s, t), (s+2, t-2), (s+4, t-4), \cdots$, we get $pa^{t+i} \cdot a^{s+1-i}q = pa^{t+j} \cdot a^{s+1-j}q$ for all i, j whenever s, t are even. But this implies that $pa^m \cdot a^nq = pa^{m+k} \cdot a^{n-k}q$ whenever $m + n$ is odd.

Now apply $R(q^{-1}a^{-1})R(a^{s+1}q) = R(q^{-1}a^0)R(a^sq)$ to $pa^{-1} \cdot a^1q = pa^0 \cdot a^0q$ to get $pa^{-1} \cdot a^{s+1}q = pa^0 \cdot a^sq$ whenever s is even. Then $L(a^1p^{-1})L(pa^{t-1}) = L(a^0p^{-1})L(pa^t)$ yields $pa^{t-1} \cdot a^{s+1}q = pa^t \cdot a^sq$ whenever s, t are even. The same argument starting from $pa^1 \cdot a^{-1}q = pa^0 \cdot a^0q$ results in $pa^{t+1} \cdot a^{s-1}q = pa^t \cdot a^sq$ whenever s, t are even. Iterating as before, we get $pa^{t+i} \cdot a^{s-i}q = pa^{t+j} \cdot a^{s-j}q$ for all i, j whenever s, t are even, which implies $pa^m \cdot a^nq = pa^{m+k} \cdot a^{n-k}q$ whenever $m + n$ is even. □

A special case of this lemma is where p, q are both powers of some element b. Now, in a flexible power alternative loop,

$$x^i(yx^j) = (y)R(x)^jL(x)^i = (y)L(x)^iR(x)^j = (x^iy)x^j \quad ,$$

so the notation x^iyx^j is unambiguous.

Lemma 3.3. *In a ARIF loop, $x^iy^m \cdot y^nx^j = x^iy^{m+n}x^j$ for all $i, j, m, n \in \mathbb{Z}$.*

Proof. We apply Lemma 3.2. $x^i \cdot yx^j = x^iy \cdot x^j$ holds by power alternativity. But also

$$x^iy^{-1} \cdot yx^j = (x^iy^{-1})(yx^{-i} \cdot x^{i+j}) = x^{i+j}$$

by the IP, and likewise $x^iy \cdot y^{-1}x^j$. □

Remark 3.4. *A commutative flexible power alternative loop which satisfies $(x^iy^m)(y^nx^j) = x^iy^{m+n}x^j$ for all $i, j, m, n \in \mathbb{Z}$ is diassociative.*

Proof. Fix a, b, and let $L = \{(a^ib^m) : i, m \in \mathbb{Z}\}$. By commutativity, $(a^ib^m)(a^jb^n) = a^{i+j}b^{m+n}$, which implies both that L is a subloop and that L is associative. □

In particular, every commutative ARIF loop is diassociative. To prove diassociativity in the non-commutative case, we set up some machinery. For a set A, let A^* be the set of finite sequences (or words) from A; i.e., A^* is the free monoid generated by A. For a word $W \in A^*$, let $|W|$ be the length

of W, so $|\,()\,| = 0$ and $|(a,b,c)| = 3$. In particular, $|\cdot| : A^* \to \mathbb{N}$ is just the unique homomorphic extension of $A \to \{1\}$. If $W, V \in A^*$, then $W^\frown V$ will denote their concatenation.

Now let L be a loop. For $B, C \subseteq L$, let $B \cdot C = \{b \cdot c : b \in B \ \&\ c \in C\}$. For a word $W \in A^*$ from some $A \subseteq L$, we wish to define the set of products of W under all possible associations. We do this inductively as follows.

Definition 3.5. *Define* $\Pi(\,()\,) = \{1\}$ *and* $\Pi((x)) = \{x\}$*, and, when* $|W| \geq 2$*:*

$$\Pi(W) = \bigcup \{\Pi(V_1) \cdot \Pi(V_2) : V_1^\frown V_2 = W \ \&\ V_1 \neq ()\ \&\ V_2 \neq ()\,\} \quad .$$

W associates *iff* $\Pi(W)$ *is a singleton.*

Alternatively, $\Pi(W)$ can be described as follows. For $A \subseteq L$, let A' be the free groupoid-with-identity on A. Let $p : A' \to A^*$ and $q : A' \to L$ be the unique homomorphic extensions of the identity map on A. Then for $W \in A^*$, $\Pi(W) = q(p^{-1}\{W\})$.

Among the products in $\Pi(W)$ is the right associated product $\pi_R(W)$ defined inductively as follows.

Definition 3.6. *Define* $\pi_R(\,()\,) = 1$ *and* $\pi_R((x)) = x$*, and, when* $|W| \geq 1$*:*

$$\pi_R((x)^\frown W) = x \cdot \pi_R(W) \quad .$$

Alternatively, for $A \subseteq L$, let $L^* : A^* \to \mathrm{Mlt}(L)$ be the unique homomorphic extension of $L : A \to \mathrm{Mlt}(L); x \mapsto L(x)$. Then the right associated product of $W \in A^*$ is $\pi_R(W) = 1L^*(W)$. W associates iff $\Pi(W) = \{\pi_R(W)\}$.

Lemma 3.7. *A loop* L *is diassociative iff for all* $a, b \in L$*, every* $W \in \{a, b, a^{-1}, b^{-1}\}^*$ *associates.*

Now, one might try to prove that all such W associate by induction on $|W|$, in which case the following definition and lemma might be helpful:

Definition 3.8. *If* $W = (a_1, \ldots a_n)$ *and* $1 \leq k \leq n-1$*, then* $\pi^k(W) = \pi_R(a_1, \ldots, a_k) \cdot \pi_R(a_{k+1}, \ldots, a_n)$

Lemma 3.9. *If* $W = (a_1, \ldots a_n)$*, then* W *associates iff:*

1. $\pi^k(W) = \pi^j(W)$ *whenever* $1 \leq j, k \leq n-1$*, and*
2. *The words* $(a_1, \ldots, a_k)$ *and* $(a_{k+1}, \ldots, a_n)$ *associate whenever* $1 \leq k \leq n-1$.

In our proof that ARIF loops are diassociative, we induct not on $|W|$, but on the *block length* of W, defined as follows:

Definition 3.10. $B(\,()\,) = 0$ *and* $B((x)) = 1$*. If* $W = (x, y)^\frown V$*, then* $B(W) = B((y)^\frown V)$ *if* $x \in \{y, y^{-1}\}$*, and* $B(W) = B((y)^\frown V) + 1$ *otherwise.*

Thus, $B(a, a, a^{-1}, b, b^{-1}, b, a) = 3$ if $a \neq b$ and $a \neq b^{-1}$.

Definition 3.11. *An IP loop* L *is* D *– associative iff for all* $a, b \in L$*, every* $W \in \{a, b, a^{-1}, b^{-1}\}^*$ *such that* $B(W) \leq D$ *associates.*

Lemma 3.12. *For any IP loop L:*

- ☞ *L is power associative iff L is 1 – associative.*
- ☞ *L is power alternative iff L is 2 – associative.*
- ☞ *L is diassociative iff L is D – associative for all D.*

So, we already know that every ARIF loop is 2 – associative.

Lemma 3.13. *Suppose that an IP loop L is $(D-1)$ – associative, and $D \geq 3$. Then L is D –* associative *iff whenever $2 \leq i \leq D-1$, $x, y \in L$, and $n, k, m_1, m_2, \ldots, m_D \in \mathbb{Z}$, the appropriate one of the following equations holds:*

$$(x^{m_1}y^{m_2}x^{m_3}\cdots y^{m_i})\cdot(y^n x^{m_{i+1}}\cdots y^{m_D}) = (x^{m_1}y^{m_2}x^{m_3}\cdots y^{m_i-k})\cdot(y^{n+k}x^{m_{i+1}}\cdots y^{m_D}) \tag{1}$$

$$(x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_i})\cdot(x^n y^{m_{i+1}}\cdots y^{m_D}) = (x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_i-k})\cdot(x^{n+k}y^{m_{i+1}}\cdots y^{m_D}) \tag{2}$$

$$(x^{m_1}y^{m_2}x^{m_3}\cdots y^{m_i})\cdot(y^n x^{m_{i+1}}\cdots x^{m_D}) = (x^{m_1}y^{m_2}x^{m_3}\cdots y^{m_i-k})\cdot(y^{n+k}x^{m_{i+1}}\cdots x^{m_D}) \tag{3}$$

$$(x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_i})\cdot(x^n y^{m_{i+1}}\cdots x^{m_D}) = (x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_i-k})\cdot(x^{n+k}y^{m_{i+1}}\cdots x^{m_D}) \tag{4}$$

i is even in (1,3) and odd in (2,4), and D is even in (1,2) and odd in (3,4).

Note that by $(D-1)$ – associativity, the parenthesized expressions in Lemma 3.13 are unambiguous. Also, note that by power alternativity, it is not necessary to consider the cases $i = 1$ and $i = D$. By Lemma 3.3,

Corollary 3.14. *Every ARIF loop is 3 – associative.*

Now, in proving D – associativity by induction on D, equations (1,2,3,4) give us four different cases to consider. Case (4) is handled easily by conjugation. First, note that 3 – associativity implies that conjugation commutes with powers:

Lemma 3.15. *In any 3 – associative IP loop, $(x^{-1}yx)^n = x^{-1}y^n x$ for all $n \in \mathbb{Z}$.*

Proof. This is clear for $n = 0$ and $n = \pm 1$, so it is sufficient to prove it for $n \geq 1$, which we do by induction on n. Assume it holds for n. By 3 – associativity, $x^{n+1} = xy \cdot y^{-1}x^n$. Let $x = u^{-1}vu = u^{-1}v^2 \cdot v^{-1}u$ and $y = u^{-1}v$. Then $xy = u^{-1}v^2$ and $x^n = u^{-1}v^n u = u^{-1}v \cdot v^{n-1}u$, so $y^{-1}x^n = v^{n-1}u$. Hence, $(u^{-1}vu)^{n+1} = x^{n+1} = xy \cdot y^{-1}x^n = u^{-1}v^2 \cdot v^{n-1}u = u^{-1}v^{n+1}u$. □

Lemma 3.16. *Suppose an IP loop L is $(D-1)$ – associative, where $D \geq 4$, and assume that $2 \leq i \leq D-1$ and D, i are both odd. Then equation (4) of Lemma 3.13 holds.*

Proof. Under the substitution $u = x^{m_1} y x^{-m_1}$, $y = x^{-m_1} u x^{m_1}$, equation (4) reduces to:

$$(u^{m_2} x^{m_3} \cdots x^{m_i+m_1}) \cdot (x^{n-m_1} u^{m_{i+1}} \cdots x^{m_D+m_1}) = \\ (u^{m_2} x^{m_3} \cdots x^{m_i+m_1-k}) \cdot (x^{n-m_1+k} u^{m_{i+1}} \cdots x^{m_D+m_1}) \quad ,$$

which is an instance of $(D-1)$ – associativity. □

Next, observe that in ARIF loops, Lemma 3.2 implies that we need only consider (1,2,3,4) in two special cases:

Lemma 3.17. *Suppose that a ARIF loop L is $(D-1)$ – associative, and $D \geq 3$. Fix i with $2 \leq i \leq D-1$, and* fix *$m_1, m_2, \ldots, m_{i-1}, m_{i+1} \ldots, m_D \in \mathbb{Z}$. Fix $x, y \in L$. Assume that the appropriate equation from (1,2,3,4) in Lemma 3.13 holds in the three special cases $m_i = k = -n = 1$, $m_i = k = -n = -1$, and $m_i = k = 1$; $n = 0$. Then the same equation holds for all values of m_i, k, n.*

Proof. For example, say D and i are even, so we are considering equation (1). Let $p = x^{m_1} y^{m_2} x^{m_3} \cdots x^{m_{i-1}}$ and let $q = x^{m_{i+1}} \cdots y^{m_D}$. Then the three special cases give us $py \cdot y^{-1} q = pq$, $py^{-1} \cdot yq = pq$, and $py \cdot q = p \cdot yq$. But then Lemma 3.2 yields (1) for all m_i, k, n. □

Actually, we shall combine the first two cases and handle $m_i = k = -n$ in Lemma 3.19. First, a preliminary lemma, which is a variant of Lemma 3.2.

Lemma 3.18. *In a ARIF loop, suppose that p, a, q, s are elements such that:*

α. $p \cdot a^m s = pa^m \cdot s \quad ; \quad s^{-1} \cdot a^m q = s^{-1} a^m \cdot q \quad ; \quad p \cdot a^m q = pa^m \cdot q \quad .$
β. $s^{-1} a^m s \cdot s^{-1} q = s^{-1} a^m q \quad .$
γ. $ps \cdot s^{-1} a^m q = pa^m s \cdot s^{-1} q = pa^m q \quad .$
δ. $pa^m s \cdot s^{-1} a^{-m} q = pq \quad .$

for all $m \in \mathbb{Z}$. Then

Δ. $pa^m s \cdot s^{-1} a^{-n} q = pa^{m-n} q$

for all $m, n \in \mathbb{Z}$.

Proof. Let $v = s^{-1} as$ and $u = s^{-1} q$. By (β) and Lemma 3.15, $v^j u = s^{-1} a^j q$ and hence $u^{-1} v^j = q^{-1} a^j s$ for every j. By Lemma 3.1, $R(v^{-n} u) = R(v^{-m} u) R(u^{-1} v^{m+k}) R(v^{-n-k} u)$ whenever k is even or $m+n$ is even. Applying this to $pa^m s$ and using (δ), we have

$$pa^m s \cdot s^{-1} a^{-n} q = [pq \cdot q^{-1} a^{m+k} s] \cdot s^{-1} a^{-n-k} q \quad .$$

But (δ) also implies that $pq = pa^{m+k} s \cdot s^{-1} a^{-m-k} q$, so by the IP we have

$$pa^m s \cdot s^{-1} a^{-n} q = pa^{m+k} s \cdot s^{-1} a^{-n-k} q \quad .$$

If k equals either $-m$ or $-n$, then this yields $pa^m s \cdot s^{-1} a^{-n} q = pa^{m-n} q$ by (γ). So, let $k = -m$ if m is even and let $k = -n$ if n is even. If m, n are both odd, then $m+n$ is even and there is no restriction on k, so k can be either $-m$ or $-n$. □

Lemma 3.19. *Suppose a ARIF loop L is $(D-1)$ – associative, where $D \geq 4$, and assume that $1 < i < D$. Then the appropriate equation (1,2,3,4) from Lemma 3.13 holds whenever $m_i = k = -n$.*

Proof. First, consider (1). When $m_i = k = -n$, this reduces to:

$$(x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_{i-1}}y^{m_i})\cdot(y^{-m_i}x^{m_{i+1}}\cdots y^{m_D}) = x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_{i-1}+m_{i+1}}\cdots y^{m_D} \quad .$$

If we let $u = y^{-m_i}xy^{m_i}$ and $x = y^{m_i}uy^{-m_i}$, then this becomes

$$(y^{m_i}u^{m_1}y^{m_2}u^{m_3}\cdots u^{m_{i-1}})\cdot(u^{m_{i+1}}\cdots y^{m_D-m_i}) = y^{m_i}u^{m_1}y^{m_2}u^{m_3}\cdots u^{m_{i-1}+m_{i+1}}\cdots y^{m_D-m_i} \quad .$$

which is an instance of $(D-1)$ – associativity. A similar argument works in cases (2) and (4) but not in case (3), where D is odd and i is even.

To illustrate case (3), consider $D = 7$ and $i = 2$, 4, or 6. If $i = 6$, we must verify

$$(x^{m_1}y^{m_2}x^{m_3}y^{m_4}x^{m_5}y^{m_6})\cdot(y^{-m_6}x^{m_7}) = x^{m_1}y^{m_2}x^{m_3}y^{m_4}x^{m_5+m_7} \quad .$$

This is no problem, since it is equivalent to

$$x^{m_1}y^{m_2}x^{m_3}y^{m_4}x^{m_5}y^{m_6} = (x^{m_1}y^{m_2}x^{m_3}y^{m_4}x^{m_5+m_7})\cdot(x^{-m_7}y^{m_6}) \quad ,$$

which is an instance of 6 – associativity. Likewise, the case $i = 2$ is no problem. But, when $i = 4$, we must verify

$$(x^{m_1}y^{m_2}x^{m_3}y^{m_4})\cdot(y^{-m_4}x^{m_5}y^{m_6}x^{m_7}) = x^{m_1}y^{m_2}x^{m_3+m_5}y^{m_6}x^{m_7} \quad .$$

This is equivalent to

$$x^{m_1}y^{m_2}x^{m_3}y^{m_4} = (x^{m_1}y^{m_2}x^{m_3+m_5}y^{m_6}x^{m_7})\cdot(x^{-m_7}y^{-m_6}x^{-m_5}y^{m_4}) \quad ,$$

which requires 8 – associativity. However, this equation requires only 6 – associativity in the special case that $m_3 = -m_5$, and this case is sufficient by Lemma 3.18, applied with $s = y^{m_4}$, $a = x$, $p = x^{m_1}y^{m_2}$, and $q = y^{m_6}x^{m_7}$. The special case is condition (δ) of Lemma 3.18, and conditions (α, β, γ) are verified using 5 – associativity.

The general situation is handled similarly. We must verify

$$(x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_{i-1}}y^{m_i})\cdot(y^{-m_i}x^{m_{i+1}}\cdots x^{m_D}) = x^{m_1}y^{m_2}x^{m_3}\cdots x^{m_{i-1}+m_{i+1}}\cdots x^{m_D} \quad ,$$

where D is odd and i is even. By mirror symmetry, we may assume that $i \geq (D+1)/2$. Fix D, i, x, y. Let $H(r)$ be the assertion that this equation holds in the special case that $m_{i+\ell} = -m_{i-\ell}$ whenever $1 \leq \ell \leq r$. So, we want to show $H(0)$. Now, $H(r)$ holds for r large enough by $(D-1)$ – associativity, and $H(r+1) \longrightarrow H(r)$ holds by Lemma 3.18, so we are done.

To be more specific, $H(r)$ asserts that

$$(x^{m_1}y^{m_2}\cdots z^{m_{i-r-2}}w^{m_{i-r-1}}z^{m_{i-r}}\cdots x^{m_{i-1}}y^{m_i})\cdot (y^{-m_i}x^{-m_{i-1}}\cdots z^{-m_{i-r}}w^{m_{i+r+1}}z^{m_{i+r+2}}\cdots x^{m_D}) = x^{m_1}y^{m_2}\cdots z^{m_{i-r-2}}\ w^{\ m_{i-r-1}+m_{i+r+1}}z^{m_{i+r+2}}\cdots x^{m_D} \quad ,$$

where (z, w) is (x, y) if r is odd and (y, x) if r is even. This is of form $db = c$, which is equivalent to $d = cb^{-1}$. Now, c has $D - 2r - 2$ blocks and b^{-1} has $D - i + 1$ blocks, and c ends with x while b^{-1} begins with x, so that the expression cb^{-1} has $2D - 2r - i - 2$ blocks, so $H(r)$ follows from $(D-1)$ – associativity whenever $2D - 2r - i - 2 \leq D - 1$, or $r \geq (D - i - 1)/2$.

Now, assume that $r \leq (D - i - 1)/2 - 1$ and assume that $H(r + 1)$ holds. $H(r + 1)$ is the special case of $H(r)$ with $m_{i+r+1} = -m_{i-r-1}$. We conclude $H(r)$ by applying Lemma 3.18, with $a = w$, $s = z^{m_{i-r}} \cdots x^{m_{i-1}} y^{m_i}$, $p = x^{m_1} y^{m_2} \cdots z^{m_{i-r-2}}$, and $q = z^{m_{i+r+2}} \cdots x^{m_D}$. Condition (δ) is $H(r+1)$, and the conclusion, (Δ), is $H(r)$. We must verify that conditions (α, β, γ) require only $(D-1)$ – associativity. (α, γ) are easy. For (β), the expression $s^{-1} w^m s s^{-1} q$ has no more than

$$(r + 1) + 1 + (r + 1) + (r + 1) + (D - i - r - 1) - 1 = D - i + 2r + 2$$

blocks. Since $2r + 2 \leq D - i - 1$ and $2i \geq D + 1$, we have

$$D - i + 2r + 2 \leq 2D - 2i - 1 \leq D - 2 \quad .$$

□

By this lemma and Lemma 3.17, the requirement for D – associativity simplifies to Lemma 3.21:

Definition 3.20. *$W(x, y; m_1, m_2, m_3, \ldots, m_D)$ denotes the word of length D, $(x^{m_1}, y^{m_2}, x^{m_3}, \ldots, z^{m_D})$, where z is x if D is odd and y if D is even*

Lemma 3.21. *Suppose a ARIF loop L is $(D-1)$ – associative, where $D \geq 4$. Then L is D – associative iff $W(x, y; m_1, m_2, m_3, \ldots, m_D)$ associates for every $x, y \in L$ and every $m_1, m_2, m_3, \ldots, m_D \in \mathbb{Z}$.*

To aid in proving this associativity:

Lemma 3.22. *Suppose a ARIF loop L is $(D-1)$ – associative, where $D \geq 4$, and $W = W(x, y; m_1, m_2, m_3, \ldots, m_D)$. Then $\pi^k(W) = \pi^{k+2}(W)$ (see Definition 3.8) whenever $1 \leq k \leq D - 3$.*

Proof. Say k is even; the argument for odd k is the same. Then we must prove

$$(x^{m_1} y^{m_2} x^{m_3} \cdots y^{m_k} x^{m_{k+1}} y^{m_{k+2}}) \cdot (x^{m_{k+3}} \cdots z^{m_D}) = (x^{m_1} y^{m_2} x^{m_3} \cdots y^{m_k}) \cdot (x^{m_{k+1}} y^{m_{k+2}} x^{m_{k+3}} \cdots z^{m_D})$$

We apply Lemma 3.2, with $p = x^{m_1} y^{m_2} x^{m_3} \cdots y^{m_k}$, $q = x^{m_{k+3}} \cdots z^{m_D}$, and $a = y^{-m_{k+2}} x^{-m_{k+1}}$. Now $p \cdot aq = pa \cdot q$ follows by $(D-2)$ – associativity, and $pa \cdot a^{-1} q = pa^{-1} \cdot aq = pq$ follows by $(D-1)$ – associativity plus Lemma 3.19. So, $p \cdot a^{-1} q = pa^{-1} \cdot q$ follows by Lemma 3.2. □

Lemma 3.23. *Suppose a ARIF loop L is $(D-1)$ – associative, where $D \geq 5$ and D is odd. Then L is D – associative.*

Proof. If $W = W(x, y; m_1, \dots, m_D)$, then Lemma 3.16 implies $\pi^2(W) = \pi^3(W)$. Thus, applying Lemma 3.22, the $\pi^k(W)$ (for $1 \leq k \leq D-1$) are all the same. It follows by Lemma 3.9 that W associates, so L is D – associative by Lemma 3.21. □

Lemma 3.24. *Suppose that a ARIF loop L is $(D-1)$ – associative, where $D \geq 4$ and D is even. Then L is D – associative.*

Proof. Again, we must show that each $W(x, y; m_1, \dots, m_D)$ associates. Let $H(r)$ be the assertion that $W(x, y; m_1, \dots, m_D)$ associates for all $x, y \in L$ and $m_1, \dots m_D \in \mathbb{Z}$ with $m_i = 1$ whenever $r < i \leq D$. So, our lemma is equivalent to $H(D)$. Let $H^+(r)$ be the assertion that $W(x, y; m_1, \dots, m_D)$ associates for all $x, y \in L$ and $m_1, \dots m_D \in \mathbb{Z}$ with $m_i = 1$ whenever $r < i < D$. So, our lemma is also equivalent to $H^+(D-1)$. We shall in fact prove:

1. $H(1)$.
2. $H(k-1) \longrightarrow H(k)$ whenever $2 \leq k \leq D-1$.
3. $H(D-1) \longrightarrow H^+(1)$.
4. $H^+(k-1) \longrightarrow H^+(k)$ whenever $2 \leq k \leq D-1$.

Applying these items in order yields $H^+(D-1)$ and hence the lemma.

First, note that, as in the proof of Lemma 3.23, $W = W(x, y; m_1, \dots, m_D)$ associates if $\pi^k(W) = \pi^{k+1}(W)$ for *some* k with $1 \leq k \leq D-2$.

To prove $H(1)$: Let $W = W(x, y; m, 1, 1, \dots, 1)$. We prove that W associates by showing that $\pi^1(W) = \pi^2(W)$; that is, $x^m \cdot yxy \cdots y = x^m y \cdot xy \cdots y$. Letting $u = xy$ so $y = x^{-1}u$, this reduces to $x^m(x^{-1}u \cdot u^{D-1}) = x^{m-1}u \cdot u^{D-1}$, which is true by 2 – associativity.

To prove $H(k-1) \longrightarrow H(k)$ when $2 \leq k \leq D$ and k is odd: W is now $(x^{m_1}, y^{m_2}, x^{m_3}, \dots, y^{m_{k-1}}, x^{m_k}, y^1, x^1 \dots y^1)$, and we shall prove that $\pi^{k-1}(W) = \pi^k(W)$. Let $p = x^{m_1}y^{m_2}x^{m_3} \cdots y^{m_{k-1}}$ and $q = y^1x^1 \cdots y^1 = y(xy)^{(D-k-1)/2}$. We need to show that $p \cdot x^{m_k}q = px^{m_k} \cdot q$. When $m_k = 1$, this is true by $H(k-1)$. But also $px \cdot x^{-1}q = px^{-1} \cdot xq = pq$ by Lemma 3.19. $H(k)$ now follows by Lemma 3.2.

The proofs for $H(k-1) \longrightarrow H(k)$ for k odd and for $H^+(k-1) \longrightarrow H^+(k)$ are the same.

Finally, we assume $H(D-1)$ and prove $H^+(1)$. Let $p = x^{m_1}(yx)^{(D-4)/2}$. We prove that $W = W(x, y; m_1, 1, 1, \dots, 1, m_D)$ associates by showing that $\pi^{D-2}(W) = \pi^{D-1}(W)$; that is, $py \cdot xy^{m_D} = pyx \cdot y^{m_D}$. By Definition 1.3 applied twice, we have $R(aba)R(b)R(a) = R(a)R(b)R(aba)$. In particular, if $a = y^{-1}$ and $b = yxy^{m_D+1}$ then $aba = xy^{m_D}$, so we get:

$$R(xy^{m_D})R(yxy^{m_D+1})R(y^{-1}) = R(y^{-1})R(yxy^{m_D+1})R(xy^{m_D}) \quad .$$

We apply this equation to $py^{-m_D}x^{-1}$:

Now, $py^{-m_D}x^{-1} \cdot xy^{m_D}$ is a product of a word with D blocks, and by Lemma 3.19, this is equal to p . Thus, applying Lemma 3.22 and power

alternativity:

$$(py^{-m_D}x^{-1})R(xy^{m_D})R(yxy^{m_D+1})R(y^{-1}) = (p \cdot yxy^{m_D+1})y^{-1} = (pyx \cdot y^{m_D+1})y^{-1} = pyx \cdot y^{m_D} \quad .$$

Likewise, $py^{-m_D}x^{-1} \cdot y^{-1}$ is a product of a word with D blocks, of form $W(x, y; m_1, 1, \cdots, 1, -m_D, -1, -1)$. This word associates by $H(D-1)$, since it is the same as $W(x, y^{-1}; m_1, -1, \cdots, 1, m_D, -1, 1)$. Thus,

$$py^{-m_D}x^{-1} \cdot y^{-1} = p \cdot y^{-m_D}x^{-1}y^{-1} = py \cdot y^{-m_D-1}x^{-1}y^{-1} \quad ;$$

the second "=" is obtained by applying Lemma 3.2, with $a = y$ and $q = x^{-1}y^{-1}$. We thus have

$$\begin{aligned}(py^{-m_D}x^{-1})R(y^{-1})R(yxy^{m_D+1})R(xy^{m_D}) &= \\ \left[(py \cdot y^{-m_D-1}x^{-1}y^{-1})(yxy^{m_D+1})\right](xy^{m_D}) &= py \cdot (xy^{m_D}) \quad ,\end{aligned}$$

and hence $H^+(1)$. □

Finally, Lemmas 3.23 and 3.24 complete the proof of Theorem 1.5.

4. Examples

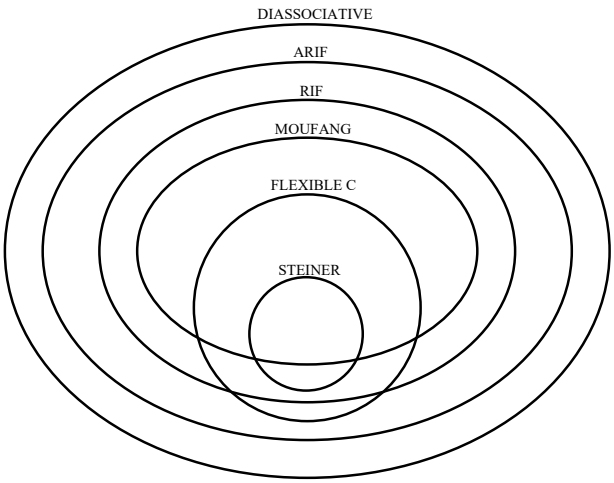

Figure 1. Some Varieties of Loops

Figure 1 depicts the sub-varieties of diassociative loops discussed in this paper. All claimed inclusions have already been proved. All regions shown are non-empty, as can easily be inferred from results in the literature plus Example 4.1: The loops which are both Moufang and Steiner are the boolean groups and clearly are a proper sub-variety of the extra loops, which are the loops which are both Moufang and (flexible) C (see Fenyves [6]), and these in turn are properly contained in the Moufang loops. If A is, say, the 10-element Steiner loop, then it is not a group and hence not Moufang. The product of A and any non-boolean group will be a RIF flexible C-loop which

is not Moufang and not Steiner. The product of A and any Moufang loop which is not an extra loop will be a RIF loop which is not a C-loop. Example 4.1 is a flexible C-loop which is not a RIF loop. Crossing this with a non-extra Moufang loop yields a ARIF loop which is neither C nor RIF. Finally, for every odd prime p, there is a diassociative loop of order p^3 which is not a group; see, e.g., the proof of Theorem 5.2 in [7]. Such loops cannot be Moufang by Chein [3], and hence not ARIF by Corollary 2.14.

Example 4.1. *There is a flexible C-loop which is not a RIF loop.*

Proof. Consider the loop in Table 1. The nucleus is $N = \{0, 1, 2\}$, and all squares are in N, so that L/N is the 8-element boolean group. This is not RIF because $(3 \cdot 12) \cdot (15 \cdot (3 \cdot 12)) \neq (3 \cdot ((12 \cdot 15) \cdot 3)) \cdot 12$, so that (3) of Lemma 2.2 fails. □

•	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21
2	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22
3	3	4	5	0	1	2	9	10	11	6	7	8	18	19	20	21	22	23	12	13	14	15	16	17
4	4	5	3	1	2	0	10	11	9	7	8	6	19	20	18	22	23	21	13	14	12	16	17	15
5	5	3	4	2	0	1	11	9	10	8	6	7	20	18	19	23	21	22	14	12	13	17	15	16
6	6	7	8	9	10	11	0	1	2	3	4	5	15	16	17	12	13	14	21	22	23	18	19	20
7	7	8	6	10	11	9	1	2	0	4	5	3	16	17	15	13	14	12	22	23	21	19	20	18
8	8	6	7	11	9	10	2	0	1	5	3	4	17	15	16	14	12	13	23	21	22	20	18	19
9	9	10	11	6	7	8	3	4	5	0	1	2	21	22	23	19	20	18	17	15	16	12	13	14
10	10	11	9	7	8	6	4	5	3	1	2	0	22	23	21	20	18	19	15	16	17	13	14	12
11	11	9	10	8	6	7	5	3	4	2	0	1	23	21	22	18	19	20	16	17	15	14	12	13
12	12	14	13	18	20	19	15	17	16	21	23	22	0	2	1	6	8	7	3	5	4	9	11	10
13	13	12	14	19	18	20	16	15	17	22	21	23	1	0	2	7	6	8	4	3	5	10	9	11
14	14	13	12	20	19	18	17	16	15	23	22	21	2	1	0	8	7	6	5	4	3	11	10	9
15	15	17	16	21	23	22	12	14	13	19	18	20	6	8	7	0	2	1	10	9	11	3	5	4
16	16	15	17	22	21	23	13	12	14	20	19	18	7	6	8	1	0	2	11	10	9	4	3	5
17	17	16	15	23	22	21	14	13	12	18	20	19	8	7	6	2	1	0	9	11	10	5	4	3
18	18	20	19	12	14	13	21	23	22	17	16	15	3	5	4	11	10	9	0	2	1	6	8	7
19	19	18	20	13	12	14	22	21	23	15	17	16	4	3	5	9	11	10	1	0	2	7	6	8
20	20	19	18	14	13	12	23	22	21	16	15	17	5	4	3	10	9	11	2	1	0	8	7	6
21	21	23	22	15	17	16	18	20	19	12	14	13	9	11	10	3	5	4	6	8	7	0	2	1
22	22	21	23	16	15	17	19	18	20	13	12	14	10	9	11	4	3	5	7	6	8	1	0	2
23	23	22	21	17	16	15	20	19	18	14	13	12	11	10	9	5	4	3	8	7	6	2	1	0

TABLE 1. A Flexible C non-RIF Loop

Example 4.2. *There is a C-loop which is not flexible.*

Proof. Consider the loop in Table 2. The nucleus is $N = \{0, 1, 2\}$, and all squares are in N, so that L/N is the 4-element boolean group. This is not flexible because $3 \cdot (6 \cdot 3) \neq (3 \cdot 6) \cdot 3$. □

•	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	0	1	2	10	11	9	8	6	7
4	4	5	3	1	2	0	11	9	10	6	7	8
5	5	3	4	2	0	1	9	10	11	7	8	6
6	6	7	8	11	9	10	0	1	2	4	5	3
7	7	8	6	9	10	11	1	2	0	5	3	4
8	8	6	7	10	11	9	2	0	1	3	4	5
9	9	10	11	7	8	6	5	3	4	0	1	2
10	10	11	9	8	6	7	3	4	5	1	2	0
11	11	9	10	6	7	8	4	5	3	2	0	1

TABLE 2. A non-Flexible C-Loop

The three examples in this section were found using the program SEM [14], which simply outputs tables, such as Tables 1 and 2. We do not see a really simple way of checking that Examples 4.1 and 4.2 are both C-loops, with the first one also flexible. However, the reader can easily write the obvious computer program (entering each loop as an array) to check these facts; it is not necessary to verify that the code for SEM itself is correct. Likewise, a program easily checks that the nucleus is $\{0, 1, 2\}$ for both loops. On the other hand, Example 4.3 below is a Steiner loop. For this one, it was easy enough to match SEM's table with the known triple systems, and then verify its properties directly from facts about such systems.

The proof of diassociativity of ARIF loops in Section 3 is by induction on the number of blocks, as is Moufang's proof for Moufang loops in [11, 12], but her proof is quite a bit shorter than ours. She first shows that whenever $(vu)w = v(uw)$, the same equation holds if the elements u, v, w are permuted or replaced by their inverses ([12], pp. 420-421). Using this fact, the step from 3 – associativity to full diassociativity is quite easy (the details are in [11]§1). Actually, as Bruck pointed out, by using this fact one can give a somewhat simpler "maximal associative set" argument which avoids mentioning blocks at all (see [1], §VII.4). However, as the following example shows, this fact does not hold in all ARIF loops, or even in all Steiner loops:

Example 4.3. *There is a Steiner loop of order 14 with elements u, v, w such that $(vu)w = v(uw)$ but $(uv)w \neq u(vw)$.*

Proof. Let $L = \mathbb{Z}_{13} \cup \{e\}$. Here, e is the identity element of the loop, so $xe = ex = x$ and $xx = e$ by definition. Products xy for distinct elements x, y of $\mathbb{Z}_{13} = \{0, 1, \ldots 12\}$ are computed in the usual way from a Steiner triple system S on $\mathbb{Z}_{13}$; that is, S is a set of 3-element subsets of $\mathbb{Z}_{13}$, and $xy = yx = z$, where z is the (unique) element of $\mathbb{Z}_{13}$ such that $\{x, y, z\} \in S$.

For S, we take one of the standard examples of a triple system (see, e.g., Example 19.12 of [9]): S contains blocks of the form $A_n = \{n, n+2, n+8\}$ and $B_n = \{n, n+3, n+4\}$, where $n \in \mathbb{Z}_{13}$.

So, for example $1 \cdot 0 = 10$ (since $B_{10} = \{10, 0, 1\}$), $10 \cdot 5 = 12$ (using A_{10}), $0 \cdot 5 = 7$ (using A_5,), and $1 \cdot 7 = 12$ (using A_{12}). Thus, $(1 \cdot 0) \cdot 5 = 1 \cdot (0 \cdot 5) = 12$.

However, $(0 \cdot 1) \cdot 5 = 12 \neq 3 = 0 \cdot (1 \cdot 5)$, since $1 \cdot 5 = 4$ (using B_1) and $0 \cdot 4 = 3$ (using B_0). □

Acknowledgement: Thanks to the referee for useful suggestions.

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1958; third printing, 1971.

[2] R.H. Bruck and L.J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) 63 (1956) 308-323.

[3] O. Chein, Moufang loops of small order. I, *Trans. Amer. Math. Soc.* 188 (1974) 31-51.

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

[5] T. Evans and B. H. Neumann, On varieties of groupoids and loops, *J. London Math. Soc.* 28 (1953) 342-350.

[6] F. Fenyves, Extra loops II. On loops with identities of Bol-Moufang type. *Publ. Math. Debrecen* 16 (1969) 187-192.

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

[8] M. K. Kinyon, K. Kunen, and J. D. Phillips, Every diassociative A-loop is Moufang, *Proc. Amer. Math. Soc.* 130 (2002) 619-624.

[9] J. H. van Lint and R. M. Wilson *A Course in Combinatorics*, Cambridge University Press, 1992.

[10] W.W. McCune, *OTTER 3.0 Reference Manual and Guide*, Technical Report ANL-94/6, Argonne National Laboratory, 1994; or see:
`http://www-fp.mcs.anl.gov/division/software/`

[11] R. Moufang, Die Desarguesschen Sätze vom Rang 10, *Math. Ann.* 108 (1933) 296-310.

[12] R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* 110 (1934) 416-430.

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

[14] J. Zhang and H. Zhang, SEM: a system for enumerating models, *Proc. 14th Int.. Joint Conf. on AI (IJCAI-95)*, Montréal, 1995, pp. 298 – 303; available at URL:
`http://www.cs.uiowa.edu/~hzhang/`

Department of Mathematics, Western Michigan University, Kalamazoo, MI 49008-5248 USA

E-mail address: `mkinyon@wmich.edu`

URL: `http://unix.cc.wmich.edu/~mkinyon`

Department of Mathematics, University of Wisconsin, Madison, WI 57306 USA

E-mail address: `kunen@math.wisc.edu`

URL: `http://www.math.wisc.edu/~kunen`

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933 USA

E-mail address: `phillipj@wabash.edu`

URL: `http://www.wabash.edu/depart/math/faculty.htm#Phillips`