Comment.Math.Univ.Carolin. 51,2 (2010) 305–317

Diassociativity is not finitely based relative to power associativity

Tomasz Kowalski

Abstract. We show that the variety of diassociative loops is not finitely based even relative to power associative loops with inverse property.

Keywords: loop, diassociativity, equational basis

Classification: Primary 08B05; Secondary 03C05, 03C20

1. Introduction

A loop is an algebra $\mathbf{L} = \langle L; \cdot, \backslash, /, e\rangle$ such that $\langle L; \cdot, e\rangle$ is a groupoid with unit, and the equivalences

$$x\backslash z = y \ \text{ iff } \ x \cdot y = z \ \text{ iff } \ x = z/y$$

hold. This is equivalent to $\mathbf{L}$ satisfying the identities

- $x(x\backslash y) = y = (y/x)x$
- $x\backslash(xy) = y = (yx)/x$

so the class of loops is a variety. The multiplication operation in loops is non-associative in general; almost equally clearly an associative loop is a group. Associativity fails in loops even for powers of a single element: an element $a \in L$ can have $a\cdot(a\cdot a) \neq (a\cdot a)\cdot a$. Evans and Neumann in [1] considered the class of *power-associative* loops, that is, those for which powers of an element are unambiguous, equivalently, such that every one-generated subloop is a group. Power-associative loops are a subvariety of loops, with an obvious infinite basis obtained by taking, for each $n \in \mathbb{N}$, all identities of the form

$$\underbrace{x\cdots x}_{n \text{ times}} = \underbrace{x\cdots x}_{n \text{ times}}$$

with different parenthesising on both sides. Evans and Neumann show that the variety of power-associative loops in not finitely based. They also make a natural next step and consider the variety of *diassociative* loops, i.e., such that every two-generated subloop is a group. Diassociative loops also have a natural infinite basis, obtained this time by parenthesising equal-length words in two letters. We will refer to such identities as *diassociative* identities. Evans and Neumann ask whether the variety of diassociative loops has a finite basis. By analogy with the power-associative case, folklore had it that the answer should be negative (cf. [2]). Yet, although certain attempts were made at providing a proof, none was deemed satisfactory.

This paper proves that the variety of diassociative loops is not finitely based even relative to power-associative loops with inverse property, thereby answering Evans and Neumann's question in the expected negative way. The proof makes use of some quite standard model theoretical results and techniques. We give [3] as the general reference for those.

2. Loops with inverse property

We will work within a subvariety of loops that is particularly group-like. Namely, if a loop $\mathbf{L}$ has the property that the left inverse e/x and right inverse $x\backslash e$ of x coincide, and moreover $x\backslash y = (x\backslash e)y$ and $y/x = y(e/x)$ hold, then we can replace the two divisions by a unary inverse and obtain a term equivalent algebra via the correspondences $x\backslash y = x^{-1}y$, $x/y = xy^{-1}$ and $x^{-1} = x\backslash e = e/x$. Thus, in this paper a loop with *inverse property*, or an *IP-loop* is an algebra $\mathbf{L} = \langle L; \cdot, ^{-1}, e\rangle$ of the type $(2, 1, 0)$ satisfying the identities

(1) $xe = x = ex$
(2) $xx^{-1} = e = x^{-1}x$
(3) $x^{-1}(xy) = y = (yx)x^{-1}$

Below we present two examples of IP-loops. The one on the left is the smallest IP-loop which is not a group, the one on the right is the smallest IP-loop which is not power-associative.

$\cdot$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	0	4	3	6	5
2	2	0	1	6	5	3	4
3	3	6	4	5	0	1	2
4	4	5	3	0	6	2	1
5	5	3	6	2	1	4	0
6	6	4	5	1	2	0	3

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	4	0	6	7	5	3
2	2	5	6	1	7	4	3	0
3	3	0	1	7	2	6	4	5
4	4	6	7	5	3	2	0	1
5	5	4	3	2	1	0	7	6
6	6	7	5	4	0	3	1	2
7	7	3	0	6	5	1	2	4

In the next section we will construct power associative IP-loops, falsifying certain diassociative identities.

3. A construction

Let p be an odd prime. Consider a function $\pi\colon \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ defined by

$$\pi(k) = \begin{cases} (p-1)k \pmod{p^2} & \text{if } k \notin \{0, p, 2p, \ldots, p(p-1)\} \\ k & \text{if } k \in \{0, p, 2p, \ldots, p(p-1)\} \end{cases}$$

so that π moves everything except multiples of p.

Lemma 1. *The function π is a permutation of $\{0,\dots,p^2-1\}$, satisfying the following conditions, for integers i,j,n,m:*

(1) $\pi^{-1}(i)=i$, *if i is a multiple of p,*
(2) $\pi^{-1}(i)=-i(p+1)$, *if i is not a multiple of p,*
(3) $\pi(-i)=-\pi(i)$ *and* $\pi^{-1}(-i)=-\pi^{-1}(i)$,
(4) $\pi(i+j)=\pi(i)+\pi(j)$ *and* $\pi^{-1}(i+j)=\pi^{-1}(i)+\pi^{-1}(j)$, *if either*
  (a) *both i and j are multiples of p, or*
  (b) *neither of i, j, $i+j$ is a multiple of p,*
(5) $\pi(\pi^{-1}(ni)-\pi^{-1}(mi))+\pi(\pi^{-1}(nj)-\pi^{-1}(mj))=\pi(\pi^{-1}(ni)-\pi^{-1}(mi)+\pi^{-1}(nj)-\pi^{-1}(mj))$, *if none of $i,j,i+j$ is a multiple of p,*

where all arithmetic operations are taken in $\mathbb{Z}_{p^2}$.

Proof: The first four statements are easily verified. For the last one, we need to consider four cases, according to whether n or m are multiples of p. To lighten the notation, let

$$\begin{aligned}\lambda&=\pi(\pi^{-1}(ni)-\pi^{-1}(mi))+\pi(\pi^{-1}(nj)-\pi^{-1}(mj))\\ \rho&=\pi(\pi^{-1}(ni)-\pi^{-1}(mi)+\pi^{-1}(nj)-\pi^{-1}(mj)).\end{aligned}$$

Case 1. p divides both n and m. Then, $\lambda=ni-mi+nj-mj=\rho$.
Case 2. p divides n but not m. Then,

$$\lambda=\pi(ni+(p+1)mi)+\pi(nj+(p+1)mj).$$

We will show that $ni+(p+1)mi$ is not a multiple of p. Suppose the contrary. Then, since $n=rp$ for some r by assumption, we get $irp+mip+mi=sp$ for some s, and therefore $mi=p(s-ir-mi)$. It follows that p divides m: a contradiction. Similarly, we get that $nj+(p+1)mj$ is not a multiple of p. Thus,

$$\begin{aligned}\lambda&=-(p+1)(ni+(p+1)mi)-(p+1)(nj+(p+1)mj)\\ &=-(p+1)(ni+(p+1)mi+nj+(p+1)mj)\\ &=-(p+1)(n(i+j)+(p+1)m(i+j))\\ &=-(p+1)(i+j)(n+(p+1)m).\end{aligned}$$

On the other hand

$$\begin{aligned}\rho&=\pi(ni+(p+1)mi+nj+(p+1)mj)\\ &=\pi(n(i+j)+(p+1)m(i+j))\\ &=\pi((i+j)(n+(p+1)m)).\end{aligned}$$

Now, reasoning as before and using the assumption that p does not divide $i+j$, it is easy to show that p does not divide $(i+j)(n+(p+1)m)$ either. Therefore,

$$\rho=-(p+1)(i+j)(n+(p+1)m)=\lambda$$

as claimed.
Case 3. p divides m but not n. By symmetry with Case 2.
Case 4. p does not divide either n or m. We have

$$\begin{aligned}\lambda &= \pi(-(p+1)(ni-mi)) + \pi(-(p+1)(nj-mj)) \\ &= \pi((p+1)i(m-n)) + \pi((p+1)j(m-n)).\end{aligned}$$

On the other hand

$$\begin{aligned}\rho &= \pi(-(p+1)(ni-mi+nj-mj)) \\ &= \pi((p+1)(i+j)(m-n)).\end{aligned}$$

But then the values of λ and ρ depend solely on whether p divides $m-n$, and $\lambda = \rho$ in either case. □

Take now the cyclic group C_{p^2} of order p^2 with g as a single generator and an element $a \notin C_{p^2}$. Let A_p be the disjoint union of C_{p^2} and $C_{p^2} \cdot a = \{g^i a \colon i \in \mathbb{Z}_{p^2}\}$. Define multiplication in A_p putting

- $g^i(g^j a) = g^{\pi(\pi^{-1}(i)+\pi^{-1}(j))} \cdot a$
- $(g^i a)g^j = g^{\pi(\pi^{-1}(i)-\pi^{-1}(j))} \cdot a$
- $(g^i a)(g^j a) = g^{\pi(\pi^{-1}(i)-\pi^{-1}(j))}$
- $g^i g^j = g^{i+j}$

Notice the similarity between this and a construction producing a (nonassociative) Moufang loop out of a (nonabelian) group. Namely, if π were identity, our construction would be identical to that construction, and thus produce an associative Moufang loop, i.e., a group.

Lemma 2. *The algebra $\mathbf{A}_p = \langle A_p; \cdot, {}^{-1}, e\rangle$ is a power associative IP-loop. Moreover, $\mathbf{A}_p$ satisfies*

(1) $(g^i g^j)g^k = g^i(g^j g^k)$
(2) $(g^i(g^j a))g^k = g^i((g^j a)g^k)$
(3) $((g^i a)g^j)(g^k a) = (g^i a)(g^j(g^k a))$
(4) $((g^i a)(g^j a))(g^k a) = (g^i a)((g^j a)(g^k a))$
(5) $(g^i(g^j a))g^i = g^j a$
(6) $((g^i a)g^j)(g^i a) = g^{-j}$
(7) $(g^i a)^{-1} = g^i a$

for all $i, j, k \in \mathbb{Z}_{p^2}$.

Proof: Straightforward calculations. □

Lemma 3. *The algebra $\mathbf{A}_p$ falsifies the identity $x^{p-1}(xy) \approx x^p y$. Thus, $\mathbf{A}_p$ is not diassociative.*

Proof: Evaluate $x \mapsto g$ and $y \mapsto a$. Then, calculate

$$g^{p-1}(ga) = g^{\pi(\pi^{-1}(p-1)+\pi^{-1}(1))} a$$

$$
\begin{aligned}
&= g^{\pi(-p(p-1)-p+1-p-1)}a\\
&= g^{\pi(-p^2-p)}a\\
&= g^{\pi(-p)}a\\
&= g^{-p}a \neq g^{p}a.
\end{aligned}
$$

□

4. Short diassociative identities

We will show that $\mathbf{A}_p$ satisfies all sufficiently short diassociative identities. Some terminology and notation first. Let X be a set of variables and $X^{-1} = \{x^{-1} \colon x \in X\}$. By a *word* we will mean a finite string of symbols from $X \cup X^{-1}$, i.e., a word over the alphabet $X \cup X^{-1}$. Thus, a *term* can be viewed as a parenthesised word. Since the identity $(xy)^{-1} = y^{-1}x^{-1}$ holds in IP-loops, each term can be reduced (over IP-loops) to one in *normal form*, that is, written in such a way that if s^{-1} is a subterm of t, then s is a variable. Let us spell it out as a lemma.

Lemma 4. *Each term t is equal over IP-loops to a term t' in normal form.*

From now on we will tacitly assume that all terms are written in normal form. For a term t, its *characteristic word* $\lfloor t \rfloor$ is the string of symbols resulting from removing all parentheses from t. Consider a word $w = x_1, \dots, x_k$. By a w-identity we mean any formal identity $t \approx s$ such that $\lfloor t \rfloor = w = \lfloor s \rfloor$. Clearly, if an IP-loop satisfies all w-identities for some word w, it is harmless to leave out parentheses in any term s whose characteristic word is a subword of w. We will do this from now on without notice.

Lemma 5. *Let $w = x_1, \dots, x_k$ be a word and $\mathbf{L}$ an IP-loop. Suppose $\mathbf{L}$ satisfies all u-identities, for any proper subword u of w. Suppose further that $\mathbf{L}$ satisfies $((x_1 \cdots x_{i-1})x_i)(x_{i+1} \cdots x_k) \approx (x_1 \cdots x_{i-1}(x_i(x_{i+1} \cdots x_k)))$ for all $i \in \{2, \dots, k-1\}$. Then $\mathbf{L}$ satisfies all w-identities.*

Proof: Consider an identity $(t(x_i \cdots x_{i+j}))s \approx t((x_i \cdots x_{i+j})s)$. Since $\mathbf{L}$ satisfies all u-identities, for any proper subword u of w, the notation above is unambiguous. Moreover, each w-identity is of the above form. We have

$$
\begin{aligned}
(t(x_i \cdots x_{i+j}))s &\approx (tx_i \cdots x_{i+j})s\\
&\approx ((tx_i \cdots x_{i+j-1})x_{i+j})s\\
&\approx (tx_i \cdots x_{i+j-1})(x_{i+j}s)\\
&\approx (tx_i \cdots x_{i+j-2})(x_{i+j-1}x_{i+j}s)\\
&\ \ \vdots\\
&\approx t(x_i \cdots x_{i+j}s)\\
&\approx t((x_i \cdots x_{i+j})s)
\end{aligned}
$$

as required. □

We recall some standard model-theoretical notions that will be of use later on. Let $\mathbf{L}$ be an IP-loop. By a *valuation* into $\mathbf{L}$ we mean any homomorphism from the absolutely free algebra of the appropriate type into $\mathbf{L}$. We will write $\mathbf{L} \models_v t \approx s$ if for a valuation v into $\mathbf{L}$ and some terms t and s we have $v(t) = v(s)$. As usual $\mathbf{L} \models t \approx s$ will mean that the identity $t \approx s$ is true in $\mathbf{L}$ (i.e., $v(t) = v(s)$ for any valuation v). We use the curly equality symbol to distinguish between formal identities (formulae) and equalities between elements of algebras. All this is typically left implicit, but since satisfying and not satisfying certain identities is what is at stake here, we state it explicitly. As a concrete example, notice that from Lemma 2 we get $\mathbf{A}_p \models x(yx) \approx (xy)x$, and moreover

$$\mathbf{A}_p \models_v xyx \approx \begin{cases} y & \text{if } v(x) = g^i \text{ and } v(y) = g^j a \\ y^{-1} & \text{if } v(x) = g^i a \text{ and } v(y) = g^j \end{cases}$$

as well as

$$\mathbf{A}_p \models_v xx \approx e \ \text{ if } \ v(x) = g^i a.$$

From Lemma 5 it now follows that to show that $\mathbf{A}_p$ satisfies all diassociative identities not longer than p, it suffices to prove that $\mathbf{A}_p \models (tx)s \approx t(xs)$, for all terms t and s in variables x and y, with $|t| + |s| < p$. Moreover, by Lemma 2(1)–(4) and symmetry, it suffices to consider only the valuations for which $t \mapsto g^i$ and $s \mapsto g^k a$.

Lemma 6. *Let t and s be terms in variables x and y. Consider a valuation v such that $v(t) = g^i$, $v(s) = g^k a$ and $v(x) = g^j$. Then $\mathbf{A}_p \models_v (tx)s \approx t(xs)$ as long as $|txs| \leq p$.*

Proof: Induction on $|txs|$. For $|txs| < 3$ the claim is trivial, and for $|txs| = 3$ it follows from Lemma 2. Suppose the claim holds for all t', s' with $|t'xs'| < n \leq p$ and take terms t and s with $|t| = \ell$, $|s| = r$ and $|txs| = n$. Observe that if $v(y) = g^m$ for any m, the claim holds trivially by associativity of C_{p^2}. Thus, we can assume $v(y) = g^m a$. By remarks preceding the lemma, we have that if xyx or yxy is a subword of either $\lfloor t \rfloor$ or $\lfloor s \rfloor$, then $\mathbf{A}_p \models_v (tx)s \approx (t'x)s'$, where t' arises from t by replacing each occurrence of xyx by y and each occurrence of yxy by x^{-1}, and s' arises similarly from s. Then, by inductive hypothesis we have $\mathbf{A}_p \models_v (t'x)s' \approx t'(xs')$ and expanding s' and t' appropriately we get the desired conclusion. Similarly, if yy is a subword of $\lfloor t \rfloor$ or $\lfloor s \rfloor$, we can shorten the terms accordingly and get access to inductive hypothesis. We can therefore assume that y occurs at most once in t and s. Further, observe that since $v(t) = g^i$, by definition of multiplication in A_p we obtain that y must occur in t an even number of times, so y cannot occur in t at all. Thus, t is of the form x^ℓ and this leaves only two choices for s, namely, $x^{r-1}y$ or yx^{r-1}. Notice also that by assumption we have $\ell + r = n - 1$.

Case 1. Let s be $x^{r-1}y$. Then $(tx)s$ is $x^{\ell+1}(x^{r-1}y)$, and $v(x^{\ell+1}(x^{r-1}y)) = g^{j(\ell+1)}(g^{j(r-1)}(g^m a))$. We then get

$$\begin{aligned} g^{j(\ell+1)}(g^{j(r-1)}(g^m a)) &= g^{j(\ell+1)}(g^{\pi(\pi^{-1}(j(r-1))+\pi^{-1}(m))} \cdot a) \\ &= g^{\pi(\pi^{-1}(j(\ell+1))+\pi^{-1}(j(r-1))+\pi^{-1}(m))} \cdot a. \end{aligned}$$

On the other hand, $t(xs) = x^\ell(x^r y)$, and calculating similarly, we obtain

$$\begin{aligned} g^{j\ell}(g^{jr}(g^m a)) &= g^{j\ell}(g^{\pi(\pi^{-1}(jr)+\pi^{-1}(m))} \cdot a) \\ &= g^{\pi(\pi^{-1}(j\ell)+\pi^{-1}(jr)+\pi^{-1}(m))} \cdot a. \end{aligned}$$

Now, to get the desired conclusion, it suffices to show that

$$\pi^{-1}(j(\ell+1)) + \pi^{-1}(j(r-1)) = \pi^{-1}(j\ell) + \pi^{-1}(jr).$$

To simplify matters even further, notice that as $1 < \ell + r = n - 1 < p$, none of ℓ, $\ell+1$, r, $r-1$ can be a multiple of p. Since p is prime, multiplying any of the above by j produces a multiple of p iff j itself is a multiple of p. Suppose j is a multiple of p. Then

$$\begin{aligned} \pi^{-1}(j(\ell+1)) + \pi^{-1}(j(r-1)) &= j(\ell+1) + j(r-1) \\ &= j(\ell+r) \\ &= j\ell + jr \\ &= \pi^{-1}(j\ell) + \pi^{-1}(jr) \end{aligned}$$

so the desired equality holds. Suppose j is not a multiple of p. Then

$$\begin{aligned} \pi^{-1}(j(\ell+1)) + \pi^{-1}(j(r-1)) &= -pj(\ell+1) - j(\ell+1) - pj(r-1) - j(r-1) \\ &= -(p+1)j(\ell+r) \\ &= -pj\ell - j\ell - pjr - jr \\ &= \pi^{-1}(j\ell) + \pi^{-1}(jr) \end{aligned}$$

and the desired equality holds again. This ends the first case.

Case 2. Let s be yx^{r-1}. Then $(tx)s$ is $x^{\ell+1}(yx^{r-1})$, and $t(xs)$ is $x^\ell(xyx^{r-1})$. For $r > 1$ we have $\mathbf{A}_p \models_v x^\ell(xyx^{r-1}) \approx x^\ell(yx^{r-2})$, so we will deal with this subcase first. Since $x^\ell(yx^{r-2})$ is strictly shorter than n, we can freely reassociate it to any form, and so we write it just as $x^\ell yx^{r-2}$. Now, since $v(xyx) = v(y)$, this further reduces to either (i) $x^{\ell-r+2}y$, if $\ell > r-2$, or (ii) $yx^{r-\ell-2}$, if $\ell < r-2$. Notice that $\ell = r-2$ is impossible, as ℓ is even and r is odd. In the case (i), we need to verify that

$$v(x^{\ell+1}(yx^{r-1})) = v(x^{\ell-r+2}y)$$

holds in $\mathbf{A}_p$. This is precisely

$$g^{\pi(\pi^{-1}(j(\ell+1))+\pi^{-1}(m)-\pi^{-1}(j(r-1)))} \cdot a = g^{\pi(\pi^{-1}(j(\ell-r+2))+\pi^{-1}(m))} \cdot a.$$

It suffices to show that the equality

$$\pi^{-1}(j(\ell+1)) - \pi^{-1}(j(r-1)) = \pi^{-1}(j(\ell-r+2))$$

holds. Suppose j is a multiple of p. We get

$$\begin{aligned}
\pi^{-1}(j(\ell+1)) - \pi^{-1}(j(r-1)) &= j(\ell+1) - j(r-1) \\
&= j\ell + j - jr + j \\
&= j(\ell - r + 2) \\
&= \pi^{-1}(j(\ell-r+2))
\end{aligned}$$

as desired. Suppose j is not a multiple of p. Then

$$\begin{aligned}
\pi^{-1}(j(\ell+1)) - \pi^{-1}(j(r-1)) &= -pj(\ell+1) - j(\ell+1) + pj(r-1) + j(r-1) \\
&= pj(r-\ell-2) + j(r-\ell-2) \\
&= (p+1)j(r-\ell-2) \\
&= -(p+1)j(\ell-r+2) \\
&= \pi^{-1}(j(\ell-r+2))
\end{aligned}$$

and this suffices. The case (ii) is rather similar. We need to verify that

$$v(x^{\ell+1}(yx^{r-1})) = v(yx^{r-\ell-2})$$

holds in $\mathbf{A}_p$. This is

$$g^{\pi(\pi^{-1}(j(\ell+1))+\pi^{-1}(m)-\pi^{-1}(j(r-1)))} \cdot a = g^{\pi(\pi^{-1}(m)-\pi^{-1}(j(\ell-r+2)))} \cdot a$$

for which it suffices to show

$$\pi^{-1}(j(\ell+1)) - \pi^{-1}(j(r-1)) = -\pi^{-1}(j(r-\ell-2))$$

but $-\pi^{-1}(j(r-\ell-2)) = \pi^{-1}(j(\ell-r+2))$, by Lemma 1(3), so the calculations from case (i) show that the required identity holds. It remains to consider the case with $r = 1$. In this case, the equality $(tx)s = t(xs)$ becomes $x^{\ell+1}y = x^{\ell}(xy)$, and this amounts to

$$g^{\pi(\pi^{-1}(j(\ell+1))+\pi^{-1}(m))} \cdot a = g^{\pi(\pi^{-1}(j\ell)+\pi^{-1}(j)+\pi^{-1}(m))} \cdot a$$

for which it suffices to show that

$$\pi^{-1}(j(\ell+1)) = \pi^{-1}(j\ell) + \pi^{-1}(j).$$

That in turn reduces to the trivial $j(\ell+1) = j\ell + j$, if j is a multiple of p, and to equally trivial $-pj(\ell+1) - j(\ell+1) = -pj\ell - j\ell - pj - j$, if j is not a multiple of p. This ends the second case and the whole proof. □

Lemma 7. *Let t and s be terms in variables x and y. Consider a valuation v such that $v(t) = g^i$, $v(s) = g^k a$ and $v(x) = g^j a$. Then $\mathbf{A}_p \models_v (tx)s \approx t(xs)$ as long as $|txs| \leq p$.*

Proof: Induction on $|txs|$ again. Suppose first that $v(y) = g^m$. Then, by the remarks preceding Lemma 6, we can replace any string of the form xx, yxy, or $xy^s x$ for some positive integer s, occurring in tx or xs, by a shorter one and gain access to the inductive hypothesis. Thus, we can assume that such strings do not occur. It follows that $t = y^\ell$ and $s = y^r$, with $\ell + r = n - 1$. Therefore $(tx)s = (g^{m\ell}(g^j a))g^{mr}$ and $t(xs) = g^{m\ell}((g^j a)g^{mr})$; the desired equality follows then by Lemma 2(3).

Now, assume $v(y) = g^m a$. As previously, all occurrences of either xx or yy can be deleted from t and s. Any such deletion shortens the term and thus enables access to inductive hypothesis. We can therefore assume further that x and y alternate in t and s. Thus, t is a sequence of alternating occurrences of $g^j a$ and $g^m a$; since $v(t) = g^i$, there must be an even number of them, so $|t|$ is even. By a similar reasoning, $|s|$ odd. We have four cases, best presented as all possible choices for the rightmost variable in t and leftmost variable in s. We will enumerate them as pairs (x, x), (x, y), (y, x) and (y, y). Notice that in the case (x, x), we can shorten both sides of $(tx)s \approx t(xs)$, thus getting access to inductive hypothesis. Further, the cases (x, y) and (y, x) are symmetric, so the number of cases reduces to two.

Case 1. Let t be $\underbrace{xy\cdots xy}_{\ell}$ and s be $\underbrace{xy\cdots x}_{r}$. We can write these, respectively, as $(xy)^{\ell/2}$ and $(xy)^{(r-1)/2}x$. Thus,

$$\begin{aligned} v(t) &= v((xy)^{\ell/2}) \\ &= g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))\ell/2} \\ &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2))} \end{aligned}$$

where the last equality follows by Lemma 1. Similarly,

$$\begin{aligned} v(s) &= v((xy)^{(r-1)/2}x) \\ &= g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))(r-1)/2}(g^j a) \\ &= g^{\pi(\pi^{-1}(j(r-1)/2)-\pi^{-1}(m(r-1)/2))}(g^j a) \\ &= g^{\pi(\pi^{-1}(j(r+1)/2)-\pi^{-1}(m(r-1)/2))} \cdot a. \end{aligned}$$

Next, we calculate

$$\begin{aligned} v(tx) &= g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))\ell/2}(g^j a) \\ &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2))}(g^j a) \\ &= g^{\pi(\pi^{-1}(j(\ell+2)/2)-\pi^{-1}(m\ell/2))} \cdot a \end{aligned}$$

and

$$\begin{aligned} v(xs) &= v(x(xy)^{(r-1)/2}x) \\ &= v((xxy(xy)^{(r-1)/2-1}x) \\ &= v((yx)^{(r-1)/2}) \\ &= g^{\pi(\pi^{-1}(m)-\pi^{-1}(j))(r-1)/2} \\ &= g^{\pi(\pi^{-1}(m(r-1)/2)-\pi^{-1}(j(r-1)/2))}. \end{aligned}$$

Finally,

$$\begin{aligned} v((tx)s) &= (g^{\pi(\pi^{-1}(j(\ell+2)/2)-\pi^{-1}(m\ell/2))}a)(g^{\pi(\pi^{-1}(j(r+1)/2)-\pi^{-1}(m(r-1)/2))}a) \\ &= g^{\pi(\pi^{-1}(j(\ell+2)/2)-\pi^{-1}(m\ell/2))-\pi^{-1}(j(r+1)/2)+\pi^{-1}(m(r-1)/2))} \end{aligned}$$

and

$$\begin{aligned} v(t(xs)) &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2))} \cdot g^{\pi(\pi^{-1}(m(r-1)/2)-\pi^{-1}(j(r-1)/2))} \\ &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2))+\pi(\pi^{-1}(m(r-1)/2)-\pi^{-1}(j(r-1)/2))} \\ &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2))+\pi(\pi^{-1}(j(1-r)/2)-\pi^{-1}(m(1-r)/2))} \\ &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2)+\pi^{-1}(j(1-r)/2)-\pi^{-1}(m(1-r)/2))} \\ &= g^{\pi(\pi^{-1}(j\ell/2)-\pi^{-1}(m\ell/2)+\pi^{-1}(m(r-1)/2)-\pi^{-1}(j(r-1)/2))} \end{aligned}$$

where the crucial penultimate equality follows from Lemma 1(5) by observing that none of $\ell/2$, $(1-r)/2$, $(\ell+1-r)/2$ is a multiple of p. Now, it suffices to show that

$$\pi^{-1}(j(\ell+2)/2) - \pi^{-1}(j(r+1)/2) = \pi^{-1}(j\ell/2) - \pi^{-1}(j(r-1)/2)$$

holds. Suppose j is a multiple of p. Then

$$\begin{aligned} \pi^{-1}(j(\ell+2)/2) - \pi^{-1}(j(r+1)/2) &= j(\ell+2)/2 - j(r+1)/2 \\ &= (j(\ell+2) - j(r+1))/2 \\ &= j(\ell+2-r-1)/2 \\ &= j(\ell-r+1)/2 \end{aligned}$$

$$
\begin{aligned}
&= (j\ell - j(r-1))/2 \\
&= j\ell/2 - j(r-1)/2 \\
&= \pi^{-1}(j\ell/2) - \pi^{-1}(j(r-1)/2)
\end{aligned}
$$

as needed. Suppose j is not a multiple of p. Then

$$
\begin{aligned}
\pi^{-1}(j(\ell+2)/2) - \pi^{-1}(j(r+1)/2) &= -(p+1)j(\ell+2)/2 + (p+1)j(r+1)/2 \\
&= (p+1)(j(r+1)/2 - j(\ell+2))/2 \\
&= (p+1)j(r+1-\ell-2)/2 \\
&= (p+1)j(r-\ell-1)/2 \\
&= -(p+1)j\ell/2 + (p+1)j(r-1)/2 \\
&= \pi^{-1}(j\ell/2) - \pi^{-1}(j(r-1)/2)
\end{aligned}
$$

precisely as required. This ends the first case.

Case 2. Let t be $\underbrace{xy\cdots xy}_{\ell}$ and s be $\underbrace{yx\cdots y}_{r}$. So, t is $(xy)^{\ell/2}$ and s is $y(xy)^{(r-1)/2}$. Then, xs can be written as $(xy)^{(r+1)/2}$. Therefore, $t(xs)$ is $(xy)^{\ell/2}(xy)^{(r+1)/2}$ and that, by power associativity, is the same as $(xy)^{(\ell+r+1)/2}$. On the other hand $(tx)s$ becomes $((xy)^{\ell/2}x)(y(xy)^{(r-1)/2})$. Therefore, we have

$$
\begin{aligned}
v(t(xs)) &= v((xy)^{(\ell+r+1)/2}) \\
&= g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))\cdot(\ell+r+1)/2}
\end{aligned}
$$

and

$$
\begin{aligned}
v((tx)s) &= v(((xy)^{\ell/2}x)(y(xy)^{(r-1)/2})) \\
&= \big(g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))\ell/2}(g^j a)\big)\big((g^m a)g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))(r-1)/2}\big) \\
&= \big(g^{\pi(\pi^{-1}(j)\cdot\ell/2-\pi^{-1}(m)\cdot\ell/2+\pi^{-1}(j))}a\big)\cdot \\
&\quad \big(g^{\pi(\pi^{-1}(m)-\pi^{-1}(j)\cdot(r-1)/2+\pi^{-1}(m)\cdot(r-1)/2)}a\big) \\
&= \big(g^{\pi(\pi^{-1}(j)\cdot(\ell+2)/2-\pi^{-1}(m)\cdot\ell/2)}a\big)\big(g^{\pi(\pi^{-1}(m)\cdot(r+1)/2-\pi^{-1}(j)\cdot(r-1)/2)}a\big) \\
&= g^{\pi(\pi^{-1}(j)\cdot(\ell+2)/2-\pi^{-1}(m)\cdot\ell/2-\pi^{-1}(m)\cdot(r+1)/2+\pi^{-1}(j)\cdot(r-1)/2)} \\
&= g^{\pi(\pi^{-1}(j)\cdot(\ell+r+1)/2-\pi^{-1}(m)\cdot(\ell+r+1)/2)} \\
&= g^{\pi(\pi^{-1}(j)-\pi^{-1}(m))\cdot(\ell+r+1)/2}.
\end{aligned}
$$

So, $v((tx)s) = v(t(xs))$ as desired. This ends the whole proof. □

The next lemma states the main result of this section.

Lemma 8. *Let $w = x_1, \dots, x_k$ be a word, with $|w| \leq p$ and $x_i \in \{x, y\}$ for $1 \leq i \leq k$. Then $\mathbf{A}_p$ satisfies all w-identities. Therefore $\mathbf{A}_p$ satisfies all diassociative identities between terms not longer than p.*

Proof: By Lemma 5, together with possible swapping of variables x and y, it suffices to show that $\mathbf{A}_p$ satisfies all w-identities of the form $t(xs) \approx (tx)s$, for some terms t and s. Let v be an arbitrary valuation. For the cases

- $v(t) = g^i$, $v(x) = g^j$, $v(s) = g^m$
- $v(t) = g^i$, $v(x) = g^j a$, $v(s) = g^m$
- $v(t) = g^i a$, $v(x) = g^j$, $v(s) = g^m a$
- $v(t) = g^i a$, $v(x) = g^j a$, $v(s) = g^m a$

the claim follows immediately by Lemma 2. Of the remaining cases

- $v(t) = g^i$, $v(x) = g^j$, $v(s) = g^m a$
- $v(t) = g^i$, $v(x) = g^j a$, $v(s) = g^m a$
- $v(t) = g^i a$, $v(x) = g^j$, $v(s) = g^m$
- $v(t) = g^i a$, $v(x) = g^j a$, $v(s) = g^m$

the first two follow, respectively, by Lemmas 6 and 7. The last two follow by symmetry with the first two. □

5. Diassociativity is not finitely based

Consider now the ultraproduct $\prod_{p \in P} \mathbf{A}_p/U$, where P is the set of odd primes and U a nonprincipal ultrafilter on P.

Lemma 9. *The algebra $\prod_{p \in P} \mathbf{A}_p/U$ is a diassociative IP-loop.*

Proof: It suffices to show that $\prod_{p \in P} \mathbf{A}_p/U$ satisfies all diassociative identities. Consider an arbitrary diassociative identity $s \approx t$, with $|s| = n = |t|$. By Lemma 8 we have $\mathbf{A}_p \models s \approx t$, for all $p \geq n$. But the set $\{p \geq n \colon p \in P\}$ is cofinite and therefore belongs to U. By properties of ultraproducts, then, $\prod_{p \in P} \mathbf{A}_p/U \models s \approx t$ as claimed. □

Recall that a class $\mathcal{K}$ of relational structures is called *elementary* if $\mathcal{K}$ is the class of models of some set Σ of first-order formulae. If Σ can be taken to be a single first-order formula, $\mathcal{K}$ is called *strictly elementary*. In particular any variety $\mathcal{V}$ of algebras is an elementary class, and if $\mathcal{V}$ is finitely based, it is strictly elementary. As a consequence of Łoś's Theorem, elementary classes are closed under ultraproducts. The following easy model-theoretical lemma will suffice for our purposes here.

Lemma 10. *Let $\mathcal{V} \subseteq \mathcal{W}$ be varieties. If $\mathcal{V}$ is finitely based relative to $\mathcal{W}$, then $\mathcal{W} \setminus \mathcal{V}$ is closed under ultraproducts.*

Proof: Let Σ be a set of equations axiomatising $\mathcal{W}$. Let ϕ be the conjunction of all equations in a finite basis of $\mathcal{V}$ relative to $\mathcal{W}$. Then, $\mathcal{W} \setminus \mathcal{V} = \mathrm{Mod}(\Sigma \cup \{\neg\phi\})$. Thus, $\mathcal{W} \setminus \mathcal{V}$ is an elementary class, hence, closed under ultraproducts. □

Armed with this, we can state our result.

Theorem 1. *The variety of diassociative IP-loops is not finitely based relative to the variety of power associative IP-loops.*

Proof: By Lemmas 9 and 10. □

Corollary 1. *The variety of diassociative IP-loops is not finitely based. Hence, neither is the variety of diassociative loops.*

Acknowledgement. I am grateful to an anonymous referee for the attention given to the paper and remarks that helped to improve the presentation greatly.

References

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

[2] Kinyon M.K., Kunen K., Phillips J.D., *A generalization of Moufang and Steiner loops*, Algebra Universalis **48** (2002), 81–101.

[3] Chang C.C., Keisler H.J., *Model Theory*, Studies in Logic and the Foundations of Mathematics, vol. 73, 3rd edition, North-Holland, Amsterdam, 1990.

University of Cagliari, Via Rockefeller 35, I-09126 Cagliari, Italy

E-mail: kowatomasz@gmail.com

(*Received* October 20, 2009, *revised* January 16, 2010)