Reza Akhtar

Linear operator identities in quasigroups

Commentationes Mathematicae Universitatis Carolinae, Vol. 63 (2022), No. 1, 1–9

Persistent URL: `http://dml.cz/dmlcz/150427`

Linear operator identities in quasigroups

Reza Akhtar

Abstract. We study identities of the form

$$L_{x_0}\varphi_1\cdots\varphi_n R_{x_{n+1}} = R_{x_{n+1}}\varphi_{\sigma(1)}\cdots\varphi_{\sigma(n)}L_{x_0}$$

in quasigroups, where $n \geq 1$, σ is a permutation of $\{1,\ldots,n\}$, and for each i, φ_i is either L_{x_i} or R_{x_i}. We prove that in a quasigroup, every such identity implies commutativity. Moreover, if σ is chosen randomly and uniformly, it also satisfies associativity with probability approaching 1 as $n \to \infty$.

Keywords: quasigroup; linear identity; associativity; commutativity

Classification: 05C78

1. Introduction

A *quasigroup* is a nonempty set G, equipped with a binary operation (written as juxtaposition), in which the left multiplication maps $L_a\colon G \to G$, $x \mapsto ax$, and the right multiplication maps $R_a\colon G \to G$, $x \mapsto xa$, are bijective for all $a \in G$. A *loop* is a quasigroup with a two sided neutral element, i.e. an element $e \in G$ such that $L_e = R_e = 1_G$, where 1_G is the identity map from G to itself. For general information on quasigroups, see [9].

When working with quasigroups, it is often convenient to work with a countably infinite set $\mathcal{X} = \{x_0, x_1, x_2, \ldots\}$ of independent indeterminates. Define sets of *left multiplication symbols* $\mathcal{L} = \{L_x\colon x \in \mathcal{X}\}$ and *right multiplication symbols* $\mathcal{R} = \{R_x\colon x \in \mathcal{X}\}$, and let $\mathcal{S} = \mathcal{L} \cup \mathcal{R}$. A *word* in $\mathcal{S}$ is a formal expression $W = \varphi_1\cdots\varphi_d$, where $d \geq 0$ and $\varphi_i \in \mathcal{S}$ for $1 \leq i \leq d$. We write $W = W(x_1,\ldots,x_m)$ to express the fact that $x_1,\ldots,x_m$ are the (distinct) indeterminates appearing in W. Such a word W is *heterogeneous* if the symbols in W are drawn from both $\mathcal{L}$ and $\mathcal{R}$, or *homogeneous* otherwise. A word $W = \varphi_1\cdots\varphi_d$ is called *alternating* if φ_i is a left multiplication symbol when i is odd and a right multiplication symbol when i is even, or vice versa. We denote by $\mathcal{S}^*$ the set of all words in $\mathcal{S}$.

We also need some notation to describe the process of substituting elements of a fixed quasigroup G for the indeterminates in a word $W \in \mathcal{S}^*$ to obtain

DOI 10.14712/1213-7243.2022.010

a map from G to itself. One might think of this process as *realizing* an abstract word in left and right multiplication symbols as an actual composition of left and right multiplication maps in G. Provided that $W = W(x_1, \ldots, x_d) = \varphi_1(x_1) \cdots \varphi_d(x_d) \in S^*$ and $a_1, \ldots, a_d \in G$, we write $W(a_1, \ldots, a_d)$ to denote the composition $\varphi_1(a_1) \cdots \varphi_d(a_d)$.

An *identity* (in $\mathcal{S}^*$) is a statement $\mathcal{I}\colon W_1 = W_2$, where $W_1, W_2 \in \mathcal{S}^*$ are words. Such an identity is called *linear* if every indeterminate present appears exactly once in each of W_1 and W_2. An identity $\mathcal{I}$ is *satisfied* in a quasigroup G if the two sides of $\mathcal{I}$ are equal upon substitution of any choice of elements of G for the indeterminates appearing in $\mathcal{I}$. By extension of terminology, we describe an identity as alternating (or heterogeneous, homogeneous) if the same is true for the words on either side for the equality symbol.

It is well-known that an associative quasigroup is in fact a group. In [8], M. Niemenmaa and T. Kepka asked which *linear identities* – that is, which equations in which each indeterminate appears exactly once on each side – imply associativity. They showed that for all $n \geq 3$, the "generalized associativity" identity

$$x_1(x_2(\ldots(x_{n-1}x_n)\ldots)) = ((\ldots(x_1x_2)\ldots)x_{n-1})x_n \tag{1}$$

is equivalent to associativity for division groupoids. A key insight in their proof is to rewrite (1) in terms of left and right multiplication maps, working, to the extent possible, with maps rather than directly with elements. In this language, the associative law is the "linear operator identity" $L_yR_z = R_zL_y$, while the commutative law is the identity $L_x = R_x$.

Questions of a similar nature, but concerning different families of identities, have been studied by A. Krapež, see [6], [7]. There are also many papers in the literature, for example, [4] and [5], concerned with functional equations on quasigroups. These papers use terminology and formalism superficially similar to that used in the present article and our past work; however, their focus is primarily on finding *operations* that satisfy functional equations of a prescribed type, whereas our focus is on studying *implications* among various equations, in the spirit of [3], [10], and [11].

Having expressed the associative law as the statement that left multiplication maps commute with right multiplication maps, there are several ways to study "map-theoretic" generalizations of it. In earlier work [1], we proved that every identity of the form

$$L_{x_1}R_{x_2}\cdots L_{x_{2n-1}}R_{x_{2n}} = R_{x_{2n}}L_{x_{2n-1}}\cdots R_{x_2}L_{x_1}, \qquad n \geq 2,$$

implies both commutativity and associativity. This was generalized further in [2], in which we studied quasigroups satisfying a *symmetric* linear operator identity, that is, an identity of the form

$$\varphi_1\varphi_2\cdots\varphi_n = \varphi_n\cdots\varphi_2\varphi_1 \tag{2}$$

in which each φ_i is either L_{x_i} or R_{x_i}. The main result of [2] is the following:

Theorem ([2, Theorem 3.1])**.** *Let $\mathcal{I}$ be a symmetric linear identity. Then*

- *$\mathcal{I}$ implies commutativity if and only if $n \geq 3$, and $\mathcal{I}$ is heterogeneous but not an alternating identity of odd length.*
- *$\mathcal{I}$ implies associativity if and only if $\mathcal{I}$ is heterogeneous and of even length.*

It is worthy of note that for $n \geq 3$, the vast majority of the 2^n identities of the form (2) imply commutativity when $n \geq 3$ is odd and *both* commutativity and associativity when n is even. It is natural, therefore, to ask if a similar result might be deduced if one does not insist upon the condition of symmetry. In particular, is it the case that given a permutation $\sigma \in S_n$, the identity $\varphi_1 \ldots \varphi_n = \varphi_{\sigma(1)} \cdots \varphi_{\sigma(n)}$ "usually" implies commutativity and/or associativity? As phrased, the question is a bit too broad to be attacked directly. However, by imposing just one condition binding the form of the identity more closely to that of the prototype $L_y R_z = R_z L_y$ that inspired these problems, we are able to prove a result of fairly broad scope. We therefore restrict consideration to identities of the form:

$$L_{x_0}\varphi_1 \ldots \varphi_n R_{x_{n+1}} = R_{x_{n+1}}\varphi_{\sigma(1)} \cdots \varphi_{\sigma(n)} L_{x_0} \tag{3}$$

in which $n \geq 2$, $x_0, \ldots, x_{n+1}$ are independent indeterminates, and φ_i is either L_{x_i} or R_{x_i} for $1 \leq i \leq n$. Our main result, see Proposition 3.1 and Corollary 3.4, is the following:

- For every $\sigma \in S_n$ the identity (3) implies commutativity.
- Suppose a permutation σ is drawn randomly and uniformly from S_n. Then (3) implies associativity with probability approaching 1 as $n \to \infty$.

We remark that the language of probability in the above statement is merely a convenience to elucidate the meaning of the result. The proofs themselves are purely combinatorial and do not draw upon any machinery from probability theory. Also, the probabilistic statement may be made more precise by examining the argument closely.

One cannot expect that the second assertion holds for *all* $\sigma \in S_n$. Since the symmetric identities (2) are subsumed under those of type (3) by taking $\sigma(i) = n - i + 1$, and alternating identities of odd length do not imply commutativity, there exist counterexamples for arbitrarily large values of n. The situation for n

even is no more hopeful; the software Mace4 found a quasigroup of order 4 in which $L_w R_x R_y R_z = R_z R_x R_y L_w$ is satisfied. From its Cayley table reproduced below, one can easily see that it is not a group.

*	0	1	2	3
0	0	2	3	1
1	2	0	1	3
2	3	1	0	2
3	1	3	2	0

The combinatorial arguments in the proof of the main theorem are rather technical, so we have relegated them to Section 2. The main results appear in Section 3.

2. Combinatorial arguments

In this section we present calculations pertaining to the symmetric group S_n. We write $f(x) = O(g(x))$ if there exists $C > 0$ such that $|f(x)| \leq C|g(x)|$ for sufficiently large x. We also write $f(x) = o(g(x))$ as $x \to \infty$ if for every $\varepsilon > 0$ there exists $N > 0$ such that $|f(x)| \leq \varepsilon |g(x)|$ for $x > N$.

For $\sigma \in S_n$, define $m(\sigma) = \gcd\{\sigma(i) - i \colon 1 \leq i \leq n,\ \sigma(i) \neq i\}$. Next, for d, $1 \leq d \leq n-1$, define $S_n^{(d)} = |\{\sigma \in S_n \colon m(\sigma) = d\}|$. Clearly S_n is partitioned by the subsets $S_n^{(d)}$, $1 \leq d \leq n-1$. Our goal is to show that $\left|S_n^{(1)}\right| = (1 - o(1))n!$, i.e. that the vast majority of permutations belong to $S_n^{(1)}$. For the balance of this section we assume n is a large integer.

Fix d as above and let $J(n) = [1, n] \cap \mathbb{Z}$. Then $I(n)$ is partitioned by the subsets $J(n,k) = \{m \in I(n) \colon m \equiv k \pmod{d}\}$, $1 \leq k \leq d$. Moreover, if $\sigma \in S_n^{(d)}$, then σ induces a permutation of each of the sets $J(n,k)$, $1 \leq k \leq d$. For convenience, let $q = \left\lfloor \frac{n}{d} \right\rfloor$ and define $r = n - qd$. Observe that

$$|J(n,k)| = \begin{cases} q+1, & 1 \leq k \leq r, \\ q, & r < k \leq d. \end{cases}$$

Lemma 2.1. *We have*

$$\frac{1}{n!} \sum_{d=2}^{n-1} |S_n^{(d)}| = o(1).$$

Proof: We will need explicit bounds associated with Stirling's approximation, see for example [12]:

$$\sqrt{2\pi}\, n^{n+1/2} \mathrm{e}^{-n} \leq n! \leq \mathrm{e} n^{n+1/2} \mathrm{e}^{-n} \tag{4}$$

and the well-known inequality

$$\mathrm{e}^x \geq 1 + x, \qquad x \geq 0. \tag{5}$$

Then

$$\bigl|S_n^{(d)}\bigr| \leq ((q+1)!)^r (q!)^{d-r} = (q!)^d (q+1)^r \leq \Bigl(\Bigl(\frac{n}{d}\Bigr)!\Bigr)^d \Bigl(\frac{n}{d}+1\Bigr)^d.$$

Applying the right inequality of (4), we have

$$\bigl|S_n^{(d)}\bigr| \leq \frac{n^{n+d/2}}{d^{n+d/2}} \mathrm{e}^{-n+d} \Bigl(\frac{n}{d}+1\Bigr)^d = (\sqrt{2\pi}\, n^{n+1/2}\mathrm{e}^{-n}) \Bigl(\frac{1}{\sqrt{2\pi}} \frac{n^{(d-1)/2}\mathrm{e}^d (n/d+1)^d}{d^{n+d/2}}\Bigr).$$

Now applying the left inequality of (4) gives

$$\bigl|S_n^{(d)}\bigr| \leq n! \Bigl(\frac{1}{\sqrt{2\pi}} \frac{n^{(d-1)/2}\mathrm{e}^d (n/d+1)^d}{d^{n+d/2}}\Bigr). \tag{6}$$

If $2 \leq d \leq 6$, (6) yields

$$\frac{1}{n!}\bigl|S_n^{(d)}\bigr| \leq \frac{1}{\sqrt{2\pi}} \frac{n^{5/2}\mathrm{e}^6 (n/2+1)^6}{2^{n+1}} = O\Bigl(\frac{n^{17/2}}{2^n}\Bigr).$$

If $7 \leq d \leq l = \lfloor \frac{n}{2} \rfloor$, we apply (5) to (6) to obtain

$$\frac{1}{n!}\bigl|S_n^{(d)}\bigr| \leq \frac{1}{\sqrt{2\pi n}} \Bigl(\frac{\mathrm{e}n^{1/2}}{d^{1/2}}\Bigr)^d \Bigl(\frac{\mathrm{e}}{d}\Bigr)^n.$$

Now it is easily checked that $F(d) = (\mathrm{e}n^{1/2}/d^{1/2})^d$ is increasing on $[0, \mathrm{e}^{n+1}]$, so in particular, $F(d) \leq F(n/2) = (2^{1/4}\mathrm{e}^{1/2})^n$. Thus

$$\frac{1}{n!}\bigl|S_n^{(d)}\bigr| \leq \frac{1}{\sqrt{2\pi n}} \Bigl(\frac{2^{1/4}\mathrm{e}^{3/2}}{d}\Bigr)^n.$$

Also,

$$\sum_{d=7}^{l} \frac{1}{d^n} \leq \int_6^\infty \frac{1}{x^n}\,\mathrm{d}x = \frac{1}{(n-1)6^{n-1}}.$$

Therefore,

$$\begin{aligned}\frac{1}{n!}\sum_{d=7}^{l}\bigl|S_n^{(d)}\bigr| &\leq \frac{1}{\sqrt{2\pi n}}(2^{1/4}\mathrm{e}^{3/2})^n \sum_{d=7}^{l}\frac{1}{d^n} \leq \frac{6}{(n-1)\sqrt{2\pi n}}\Bigl(\frac{2^{1/4}\mathrm{e}^{3/2}}{6}\Bigr)^n \\ &= O\Bigl(\frac{(8/9)^n}{n^{3/2}}\Bigr).\end{aligned}$$

Finally, when $l+1 \le d \le n-1$, then $\sigma \in S_n^{(d)}$ only if σ is a product of no more than $n-d$ transpositions of the form $(i\ i+d)$. Thus $|S_n^{(d)}| \le 2^{n-d}$, and so

$$\frac{1}{n!}\sum_{d=l+1}^{n-1} \left|S_n^{(d)}\right| \le \frac{2^{n/2+1}}{n!} = O\left(\frac{1}{\sqrt{n}}\left(\frac{\sqrt{2}\mathrm{e}}{n}\right)^n\right)$$

by (4). Collecting all these bounds together, we conclude $\frac{1}{n!}\sum_{d=2}^{n-1}\left|S_n^{(d)}\right| = o(1)$. □

Corollary 2.2. *Suppose a permutation σ is drawn randomly and uniformly from S_n. Then $\sigma \in S_n^{(1)}$ with probability* $1 - o(1)$.

3. Results

Throughout this section, we assume $x_0, \dots, x_{n+1}$ are independent indeterminates.

Proposition 3.1. *Let $\sigma \in S_n$, and suppose φ_i is either L_{x_i} or R_{x_i} for $1 \le i \le n$. Then every quasigroup satisfying an identity of the form*

$$L_{x_0}\varphi_1 \cdots \varphi_n R_{x_{n+1}} = R_{x_{n+1}}\varphi_{\sigma(1)} \cdots \varphi_{\sigma(n)} L_{x_0} \tag{7}$$

is commutative.

Proof: For convenience, write $W(x_1,\dots,x_n) = \varphi_1 \cdots \varphi_n$ and $W'(x_1,\dots,x_n) = \varphi_{\sigma(1)} \cdots \varphi_{\sigma(n)}$ so that the identity reads

$$L_{x_0}W(x_1,\dots,x_n)R_{x_{n+1}} = R_{x_{n+1}}W'(x_1,\dots,x_n)L_{x_0}. \tag{8}$$

Let G be a quasigroup in which the above identity is satisfied, and suppose $a \in G$. By [2, Corollary 2.2], there exist $b_1,\dots,b_n \in G$ such that $L_aW(b_1,\dots,b_n) = 1_G$ and $R_aW'(b_1,\dots,b_n) = 1_G$. Substituting $x_0 = x_{n+1} = a$ and $x_i = b_i$ for $1 \le i \le n$ into (8), we deduce $R_a = L_a$. □

Proposition 3.2. *Suppose a quasigroup G satisfies* (7) *and $\sigma \in S_n^{(1)}$. Then G is a loop.*

Proof: Fix $a \in G$. Since R_a is surjective, there exists $e \in G$ such that $R_ae = a$, i.e. $ea = a$. By Proposition 3.1, G is commutative, so to show that e is a neutral element it suffices to prove $L_e = 1_G$. Again, by commutativity we may rewrite (7) as

$$L_{x_0}L_{x_1} \cdots L_{x_n}L_{x_{n+1}} = L_{x_{n+1}}L_{x_{\sigma(1)}} \cdots L_{x_{\sigma(n)}}L_{x_0}. \tag{9}$$

Now suppose $b \in G$, and select $c \in G$ such that $ca = b$. For every i_0, $1 \le i_0 \le n$, substitute

$$x_i = \begin{cases} c, & i = i_0, \\ e, & i \neq i_0, \end{cases}$$

into (9) to obtain

$$L_e^{i_0} L_c L_e^{n-i_0} = L_e^{\sigma^{-1}(i_0)} L_c L_e^{n-\sigma^{-1}(i_0)}.$$

Applying both sides to the element a, we deduce $L_e^{i_0}(ca) = L_e^{\sigma^{-1}(i_0)}(ca)$, i.e. $L_e^{i_0-\sigma^{-1}(i_0)} b = b$. This equality holds for all i_0, $1 \le i_0 \le n$, but is vacuous when $\sigma^{-1}(i_0) = i_0$.

Let $I = \{i_0 \colon \sigma^{-1}(i_0) \neq i_0\} = \{i_0 \colon \sigma(i_0) \neq i_0\}$. Then, because $\sigma \in S_n^{(1)}$, $m(\sigma) = \gcd(i_0 - \sigma^{-1}(i_0))_{i_0 \in I} = \gcd(\sigma(i_0) - i_0)_{i_0 \in I} = 1$, and so we conclude $L_e b = b$. Since $b \in G$ was arbitrary, $L_e = 1_G$. □

Corollary 3.3. *Suppose a quasigroup G satisfies (7) and $\sigma \in S_n^{(1)}$. Then G is an abelian group.*

Proof: By Proposition 3.1, G is commutative, and by Proposition 3.2 there exists $e \in G$ such that $L_e = R_e = 1_G$. Substituting $x_1 = \ldots = x_n = e$ into (7) we obtain $L_{x_0} R_{x_{n+1}} = R_{x_{n+1}} L_{x_0}$, which is precisely the associative law. □

In view of Lemma 2.1 we therefore have:

Corollary 3.4. *Suppose a permutation σ is drawn randomly and uniformly from S_n. Then with probability $1 - o(1)$, any quasigroup satisfying (7) is an abelian group.*

The referee has pointed out that Corollary 3.3 has a partial converse:

Proposition 3.5. *Suppose $\sigma \in S_n$ and $r = \gcd(m(\sigma), n+1) \ge 2$. Then there exists a nonassociative quasigroup in which (7) holds.*

Proof: Suppose the prime factorization of r is $2^e \cdot p_1^{e_1} \cdots p_s^{e_s}$, where the p_i are distinct odd primes, and let $Q = \mathbb{Z}_{2^{e+2}} \times \mathbb{Z}_{p_1^{e_1+1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s+1}}$. Then Q, considered as an abelian group, has an automorphism φ of order r. Define a quasigroup structure "$\cdot$" on Q by $x \cdot y = \varphi(x+y)$. Then $(Q, \cdot)$ is clearly commutative. If Q were associative, then the identity $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ would imply $\varphi(x) + \varphi^2(y) + \varphi^2(z) = \varphi^2(x) + \varphi^2(y) + \varphi(z)$, i.e. $\varphi(x-z) = \varphi^2(x-z)$, forcing $\varphi = 1_Q$. Thus, Q is not associative. In view of commutativity, the identity (7) reads

$$L_{x_0} L_{x_1} \cdots L_{x_n} L_{x_{n+1}} = L_{x_{n+1}} L_{x_{\sigma(1)}} \cdots L_{x_{\sigma(n)}} L_{x_0}. \tag{10}$$

In $(Q, \cdot)$, the left hand side of (10) applied to an indeterminate y reads

$$\varphi(x_0) + \sum_{i=1}^{n} \varphi^{i+1}(x_i) + \varphi^{n+2}(x_{n+1}) + \varphi^{n+2}(y) \tag{11}$$

while the right hand side reads

$$\varphi(x_{n+1}) + \sum_{i=1}^{n} \varphi^{i+1}(x_{\sigma(i)}) + \varphi^{n+2}(x_0) + \varphi^{n+2}(y). \tag{12}$$

From the definition, we see that r divides $\sigma(i) - i$ for i, $1 \leq i \leq n$. Therefore, if $j = \sigma(i)$, then $\varphi^{j+1}(x_j) = \varphi^{\sigma(i)+1}(x_{\sigma(i)}) = \varphi^{i+1}(x_{\sigma(i)})$. Moreover, since r divides $n+1$, we have $\varphi^{n+1} = 1_Q$, so

$$\begin{aligned} &\varphi(x_0) + \sum_{i=1}^{n} \varphi^{i+1}(x_i) + \varphi^{n+2}(x_{n+1}) + \varphi^{n+2}(y) \\ &\qquad = \varphi^{n+2}(x_0) + \sum_{i=1}^{n} \varphi^{i+1}(x_{\sigma(i)}) + \varphi(x_{n+1}) + \varphi^{n+2}(y). \end{aligned}$$

Thus (10) and hence also (7) holds in $(Q, \cdot)$. □

Acknowledgement. We thank the referee for comments that helped improve this paper.

References

[1] Akhtar R., *On generalized associativity in groupoids*, Quasigroups Related Systems **24** (2016), no. 1, 1–6.

[2] Akhtar R., *Symmetric linear operator identities in quasigroups*, Comment. Math. Univ. Carolin. **58** (2017), no. 4, 401–417.

[3] Akhtar R., Arp A., Kaminski M., Van Exel J., Vernon D., Washington C., *The varieties of Bol–Moufang quasigroups defined by a single operation*, Quasigroups Related Systems **20** (2012), no. 1, 1–10.

[4] Belousov V. D., *Systems of quasigroups with generalized identities*, Uspehi Mat. Nauk **20** (1965), no. 1 (121), 75–146 (Russian).

[5] Krapež A., *Generalized linear functional equations on almost quasigroups. I. Equations with at most two variables*, Aequationes Math. **61** (2001), no. 3, 255–280.

[6] Krapež A., *Quadratic level quasigroup equations with four variables. I*, Publ. Inst. Math. (Beograd) (N.S.) **81 (95)** (2007), 53–67.

[7] Krapež A., *Quadratic level quasigroup equations with four variables. II: The lattice of varieties*, Publ. Inst. Math. (Beograd) (N.S.) **93 (107)** (2013), 29–47.

[8] Niemenmaa M., Kepka T., *On a general associativity law in groupoids*, Monatsh. Math. **113** (1992), no. 1, 51–57.

[9] Pflugfelder H., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics, 7, Heldermann, Berlin, 1990.

[10] Phillips J. D., Vojtěchovský P., *The varieties of loops of Bol–Moufang type*, Algebra Universalis **54** (2005), no. 3, 259–271.

[11] Phillips J. D., Vojtěchovský P., *The varieties of quasigroups of Bol–Moufang type: an equational reasoning approach*, J. Algebra **293** (2005), no. 1, 17–33.

[12] Robbins H., *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.

R. Akhtar:
Department of Mathematics, Miami University, 501 E High St, Oxford, Ohio, OH 45056, USA

E-mail: akhtarr@miamioh.edu

(*Received* December 31, 2020*, revised* December 16, 2021)