PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 105(119) (2019), 17–24 DOI: https://doi.org/10.2298/PIM1919017K

WEAK ASSOCIATIVITY AND QUASIGROUP UNITS

Aleksandar Krapež

Abstract. We investigate a family of identities similar to weak associativity: $x(y/y)\cdot z = x\cdot(y/y)z$ which might imply the existence of the {left, right, middle} unit in a quasigroup. A partial solution to Krapež, Shcherbacov Problem concerning such identities and consequently to similar well known Belousov's Problem is obtained. Another problem by Krapež and Shcherbacov is solved affirmatively, showing that there are many single identities determining unipotent loops among quasigroups.

1. Introduction

We concern ourselves with the old problem of Belousov [**1**]:

Problem 1.1. *How to recognize identities which force quasigroups satisfying them to be loops?*

and its generalization:

Problem 1.2 (Krapež, Shcherbacov [**10**]). *How to recognize identities which force quasigroups satisfying them to have the {left, right, middle} unit?*

There are many results relevant to these two problems. See [**10**] and the references given there. For example, the important identity of associativity as well as Moufang and Bol identities are all known to be particular solutions of Problems 1.1 and/or 1.2. However, these problems are not solved in general. We give here one family of solutions based on the result by Smith [**17**] and its generalization by Krapež and Shcherbacov [**10**]

2. Quasigroups

Eighty years did pass from the moment when quasigroups were defined for the first time (Moufang [**14**]). But the interest in them is strong and growing steadily. Some of it comes from the well established connections to combinatorics

2010 *Mathematics Subject Classification:* Primary 20N05.
Key words and phrases: quasigroup, loop, unit, weak associativity.
Communicated by Žarko Mijajlović.

(the Cayley table of a quasigroup is *latin square*; *Steiner quasigroups* and *Steiner loops* generate *Steiner triple systems* – see Evans [**4**]) and to geometry (3-*nets* can be coordinatized by quasigroups – see Belousov [**2**]). But it also comes from applications in statistics (the theory of experimental design – Fisher [**6**]), physics (the theory of relativity – Ungar [**18**]) and in particular from its increasing use in cryptography (see for example Kościelny [**7**], Markovski [**12**, **13**], Krapež [**8**], Shcherbacov [**16**], Krömer et al. [**11**]). The recent introduction of *fuzzy quasigroups* (Krapež, Šešelja, Tepavčević [**9**]) enables applications in engineering where fuzzy mathematics is used.

* * *

Of the two usual ways to define quasigroups we choose the one which treats them as algebras with three binary operations. A few related weaker algebras are also defined. Basic facts about quasigroups can be found in Belousov [**1**], Pflugfelder [**15**], Chein, Pflugfelder, Smith [**3**], Shcherbacov [**16**]. We expect the reader to be familiar with just the few elementary results needed (see [**10**]).

Definition 2.1. An algebra $(Q; F, G)$ is a *left quasigroup* if it satisfies:

$$xF(xGy) = y \quad \text{and} \quad xG(xFy) = y.$$

An algebra $(Q; F, H)$ is a *right quasigroup* if it satisfies:

$$(xHy)Fy = x \quad \text{and} \quad (xFy)Hy = x.$$

An algebra $(Q; F, G, H)$ is a *quasigroup* if $(Q; F, G)$ is left and $(Q; F, H)$ is right quasigroup.

If we have a (left, right) quasigroup we say that F is a *(left, right) quasigroup operation*. Moreover, we conveniently say that groupoid $(Q; F)$ is a quasigroup if the operation F is a quasigroup operation. There is no harm in that if we keep in mind that groupoid $(Q; F)$ and algebra $(Q; F, G, H)$ have different properties. For example, the class of all quasigroups is a variety while the class of all groupoids with quasigroup operations is not.

Often, we write $G = F^{-1}$, $H = {}^{-1}F$ for these, so called *inverse operations* of F. The operation $G = F^{-1}(H = {}^{-1}F)$ exists if and only if F is left (right) quasigroup operation and then $G(H)$ is also a left (right) quasigroup operation.

Definition 2.2. A groupoid $(Q; F)$ is a *left (right) cancellation* groupoid, iff $aFx = aFy \Rightarrow x = y$ ($xFa = yFa \Rightarrow x = y$) for all $a, x, y \in Q$.

When we use multiplicative notation (i.e., if operations $\cdot, \backslash, /$ correspond to F, G, H respectively), we also use the customary symbols: $*, \backslash, /, /\!\!/, \backslash\!\!\backslash$ for *parastrophes* of $\cdot$:

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

In this case the quasigroup axioms take the more familiar form:

$$x\backslash xy = y \qquad xy/y = x$$
$$x(x\backslash y) = y \qquad (x/y)y = x.$$

It will be usefull to define three partitions of the set $\Pi = \{\cdot, *, /, \backslash, /\!/, \backslash\!\backslash\}$ of all parastrophes of $\cdot$.

Definition 2.3. The partitions are given in the following table:

	1^{st} class	2^{nd} class	3^{rd} class
The first partition:	$\lambda = \{*, \backslash\!\backslash\}$	$\rho = \{\cdot, /\}$	$\mu = \{\backslash, /\!/\}$
The second partition:	$L = \{/, /\!/\}$	$R = \{\backslash, \backslash\!\backslash\}$	$M = \{\cdot, *\}$
The third partition:	$\ell = \{\cdot, \backslash\}$	$r = \{*, /\!/\}$	$m = \{/, \backslash\!\backslash\}$

* * *

The definition of various types of units is conveniently collected in the Table 1. The alternative definitions may be formulated either in the language $\{\cdot, e\}$ of groupoids with constant (indicated by (1)) or in the language of quasigroups (indicated by (3)).

Table 1. Units in quasigroups

Unit	Symbol	Identities (1)	Identities (3)
none	(Q)	$x = x$	$x = x$
left	(eQ)	$ex = x$	$x/x = y/y$
right	(Qe)	$xe = x$	$x\backslash x = y\backslash y$
middle	(U)	$xx = e$	$xx = yy$
ℓ + r	(Q1)	$ex = x, xe = x$	$x/x = y\backslash y$
ℓ + m	(eU)	$ex = x, xx = e$	$x/x = yy$
r + m	(Ue)	$xe = x, xx = e$	$x\backslash x = yy$
ℓ + r + m	(U1)	$ex = x, xe = x, xx = e$	$x/x = y\backslash y = zz$

Definition 2.4. A quasigroup $(Q; \cdot, \backslash, /)$ is:

- A *left (right) loop* if $(Q; \cdot)$ has a left (right) unit.
- An *unipotent quasigroup* if $(Q; \cdot)$ has a middle unit.
- A *loop* if it has both left and right units.
- An *unipotent left (right) loop* if it has left (right) and middle units.
- An *unipotent loop* if it has left, right and middle units.

The following result is well known:

Theorem 2.1. *Any {left, right, middle} unit of a quasigroup $(Q; \cdot, \backslash, /)$ is its unique idempotent.*

We see that an operation $\cdot$ has a unit iff $\backslash$ and $/$ are both unipotent, i.e., they have the (common) middle unit. Similar connections between different kinds of units in various parastrophes of a quasigroup $(Q; \cdot)$ are given in the Table 2 (see also [**10**]).

TABLE 2. Units of parastrophic operations

$\cdot$	$*$	$/$	$\backslash$	$\backslash\backslash$	$//$
ℓ	r	m	ℓ	r	m
r	ℓ	r	m	m	ℓ
m	m	ℓ	r	ℓ	r

For example, the entry m in the row r and the column $\backslash\backslash$ of Table 2, means that the middle unit e of the operation $\backslash\backslash$ ($x\backslash\backslash x = e$) is the right unit of the operation $\cdot$ ($x \cdot e = x$).

We see that every type of quasigroup from Table 1 may be defined by the single identity. The only exceptions are unipotent loops which require two identities. Krapež and Shcherbacov posed the related problem in [**10**]:

PROBLEM 2.1. *Is there a single identity (in the language $\{\cdot, \backslash, /\}$) which defines unipotent loops among quasigroups?*

Problem 2.1 is solved in Section 3 and, independently, in Fempl-Mađarević, Krapež [**5**].

All lattices of classes of quasigroups, defined above in one of the two languages mentioned, are isomorphic to the *generic lattice* given in Figure 1.

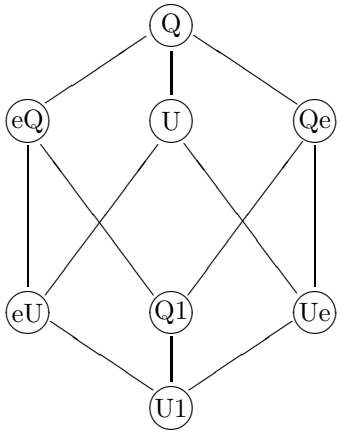

FIGURE 1. Generic lattice of classes of quasigroups

3. The identity $(xA(yBy))Cz = xC((yDy)(^{-1}D)z)$

Smith proved in [**17**, Proposition 1.3]:

THEOREM 3.1. *A nonempty quasigroup $(Q, \cdot, \backslash, /)$ is a loop iff*

$$x(y/y) \cdot z = x \cdot (y/y)z.$$

Krapež and Shcherbacov used this theorem and internal symmetry of quasigroups to give five more similar results in [**10**]:

THEOREM 3.2. *A nonempty quasigroup $(Q, \cdot, \backslash, /)$ is a loop iff*

$$x(y\backslash y)\cdot z = x\cdot(y\backslash y)z.$$

A nonempty quasigroup $(Q, \cdot, \backslash, /)$ is an unipotent left loop iff any of:

$$(x\backslash yy)\backslash z = x\backslash(yy\backslash z)$$
$$(x\backslash(y/y))\backslash z = x\backslash((y/y)\backslash z).$$

A nonempty quasigroup $(Q, \cdot, \backslash, /)$ is an unipotent right loop iff any of:

$$(x/yy)/z = x/(yy/z)$$
$$(x/(y\backslash y))/z = x/((y\backslash y)/z).$$

We generalize both these statements:

THEOREM 3.3. *Let $(Q;A)$ be a left quasigroup, $(Q;B)$ a groupoid, $(Q;C)$ a cancellative groupoid and let $(Q;D)$ be a right quasigroup. If they satisfy the identity*

$$(xA(yBy))Cz = xC((yDy)(^{-1}D)z) \tag{WA}$$

then there are $e, i \in Q$ such that:

- *e is the right unit for A,*
- *e is the middle unit for B,*
- *i is the middle unit for D.*

The converse also holds.

PROOF. 1) Assume that e is the right unit for A and the middle unit for B, while i is the middle unit for D. Then $xAe = x$, $yBy = e$ and $yDy = i$, which implies $i(^{-1}D)z = z$. Replacing, we get $(xA(yBy))Cz = (xAe)Cz = xCz = xC(i(^{-1}D)z) = xC((yDy)(^{-1}D)z)$.

2) Conversely, let a left quasigroup $(Q;A)$, a groupoid $(Q;B)$, a cancellative groupoid $(Q;C)$ and a right quasigroup $(Q;D)$ satisfy identity (WA).

2a) Replace z in (WA) by y. We get $(xA(yBy))Cy = xC((yDy)(^{-1}D)y)$. As D is a right quasigroup, we get $(xA(yBy))Cy = xCy$. Since C is cancellative, we reduce it to $xA(yBy) = x$. Using the fact that A is a left quasigroup, we finally get $xA^{-1}x = yBy$. This implies that A^{-1} and B have the common middle unit, say e. It also follows that e is right unit for A.

2b) Since e is middle unit of B and right unit of A, we have $(xA(yBy))Cz = (xAe)Cz = xCz$. Therefore $xCz = xC((yDy)(^{-1}D)z)$. However, C is cancellative and we may cancel from the left to get $z = (yDy)(^{-1}D)z$. Since D is a right quasigroup, it follows that $yDy = zDz$ proving D unipotent. Therefore, D has a middle unit i. □

We are particularly interested in the case where A, B, C, D are parastrophes of the same quasigroup $(Q;\cdot)$. This has two immediate consequences:

- All four operations are quasigroups;

- The existence of unit e for A, B and i for D implies (Theorem 2.1) that $i = e$ is some kind of unit in $(Q; \cdot)$ (see Table 2).

On the contrary, the choice of C does not impose any restriction on $\cdot$, therefore we can choose C arbitrarily.

Let us try to describe all cases that may happen for various choices of A, B, C, D. There are $6^4 = 1296$ possible cases. Every choice of $(A, B, C, D) \in \Pi^4$ makes (WA) equivalent to one of $(eQ), (Qe), (U), (Q1), (eU), (Ue), (U1)$.

The utility of partitions given in the Definition 2.3 now becomes apparent:

LEMMA 3.1. *If $\{A \in \lambda, A \in \rho, A \in \mu\}$ then the quasigroup $(Q; \cdot)$ has a {left, right, middle} unit.*

PROOF. Use Table 2. □

Analogously:

LEMMA 3.2. *Let F denote one of the operations B or D. If $\{F \in L, F \in R, F \in M\}$ then the quasigroup $(Q; \cdot)$ has a {left, right, middle} unit.*

It is easy now to distinguish the tuples (A, B, C, D) of parastrophes of $\cdot$ which force $(Q; \cdot)$ to have the left (and only left!) unit:

THEOREM 3.4. *$((\mathrm{WA}) \Leftrightarrow (eQ))$ iff $A \in \lambda, B \in L, C \in \Pi, D \in L$.*

PROOF. By Theorem 3.3, the tuple (A, B, C, D) satisfies (WA) iff there is an element $e \in Q$ such that $xAe = x, xBx = e, xDx = e$. All three identities are equivalent to $e \cdot x = x$ (i.e., to (eQ)) iff $A \in \lambda, B \in L, D \in L$. The statement of the Theorem follows. □

Consequently, there are $48 = 6 \times 2^3$ instances of (WA) equivalent to (eQ).

We can introduce a short notation for the conditions on tuples:

DEFINITION 3.1. Let $\omega \in \{\lambda, \rho, \mu\}$, $X, Y \in \{L, R, M\}$ and $w \in \{\ell, r, m\}$.

- ωXY is defined to mean $A \in \omega$, $B \in X$, $C \in \Pi$, $D \in Y$.
- XwY is defined to mean $E \in \Pi$, $F \in X$, $G \in w$, $H \in Y$.

Theorem 3.4 may be written now as: (WA) $\Leftrightarrow (eQ))$ iff λLL.

Analogously, there are 48 (WA)-identites equivalent to (Qe) (resp. (U)):

THEOREM 3.5. (1) *$((\mathrm{WA}) \Leftrightarrow (Qe))$ iff ρRR.* (2) *$((\mathrm{WA}) \Leftrightarrow (U))$ iff μMM.*

Similarly, there are $288 = 6 \times 48$ identities equivalent to (Q1) (resp. (eU), (Ue), (U1)):

THEOREM 3.6. *We have*

(1) *$((\mathrm{WA}) \Leftrightarrow (Q1))$ iff exactly one of: $\lambda LR, \lambda RL, \lambda RR, \rho LL, \rho LR, \rho RL$.*
(2) *$((\mathrm{WA}) \Leftrightarrow (eU))$ iff exactly one of: $\lambda LM, \lambda ML, \lambda MM, \mu LL, \mu LM, \mu ML$.*
(3) *$((\mathrm{WA}) \Leftrightarrow (Ue))$ iff exactly one of: $\mu MR, \mu RM, \mu RR, \rho MM, \rho MR, \rho RM$.*
(4) *$((\mathrm{WA}) \Leftrightarrow (U1))$ iff exactly one of: $\lambda MR, \lambda RM, \mu LR, \mu RL, \rho LM, \rho ML$.*

Theorem 3.6, item (4) gives us 288 solutions of Problem 2.1. One of them is presented in the following example.

Example 3.1. Let us consider the identity:

$$((x/x)/y)z = y(z/(x\backslash x)). \tag{3.1}$$

Using parastrophic operations we may write (3.1) in the form:

$$(y/\!\!/(x/x))z = y((x\backslash x)/\!\!/z). \tag{3.2}$$

It is a special case of WA–identity with $A = /\!\!/, B = /, C = \cdot, D = \backslash$. It follows that $A \in \mu$, $B \in L$, $D \in R$. By Theorem 3.6 identity (3.2) (therefore (3.1)) is equivalent to $(U1)$.

4. The identity $xE((yFy)Gz) = (xH^{-1}(yHy))Ez$

Let us consider the identity

$$xE((yFy)Gz) = (xH^{-1}(yHy))Ez. \tag{4.1}$$

It looks similar to (WA) and the first idea is to use the same methods (under appropriate conditions on E, F, G, H) as were used in Theorem 3.3. The idea is sound and can be carried out, but there is an easier way as we shall show proving the following:

Theorem 4.1. *Let $(Q; E)$ be a cancellative groupoid, $(Q; F)$ be a groupoid, $(Q; G)$ be a right quasigroup and let $(Q; H)$ be a left quasigroup. If they satisfy the identity* (4.1) *then there are $e, i \in Q$ such that:*

- *e is the middle unit for F*
- *e is the left unit for G*
- *i is the middle unit for H.*

The converse also holds.

Proof. Let us make a sequence of equivalent transformations of (4.1):

$$((yFy)Gz)E^*x = zE^*(xH^{-1}(yHy))$$

$$(zG^*(yFy))E^*x = zE^*((yH^*y)(H^{-1})^*x)$$

and, because of $(H^{-1})^* = {}^{-1}(H^*)$:

$$(zG^*(yFy))E^*x = zE^*((yH^*y)({}^{-1}(H^*))x)$$

which is (WA) for $A = G^*, B = F, C = E^*, D = H^*$. By Theorem 3.3 there are $e, i \in Q$ such that: $G^*(x, e) = x, F(x, x) = e$ and $H^*(x, x) = i$ which is exactly what is needed.

The converse holds by direct computation. □

The following lemma is analogous to Lemmas 3.1 and 3.2.

Lemma 4.1. *If $\{G \in \ell, G \in r, G \in m\}$ then the quasigroup $(Q; \cdot)$ has a {left, right, middle} unit.*

We can prove now:

Corollary 4.1. *We have:*

(1) $((4.1) \Leftrightarrow (eQ))$ *iff* $L\ell L$

(2) $((4.1) \Leftrightarrow (Qe))$ *iff* RrR
(3) $((4.1) \Leftrightarrow (U))$ *iff* MmM
(4) $((4.1) \Leftrightarrow (Q1))$ *iff exactly one of:* $L\ell R, LrL, LrR, R\ell L, R\ell R, RrL$
(5) $((4.1) \Leftrightarrow (eU))$ *iff exactly one of:* $L\ell M, LmL, LmM, M\ell L, M\ell M, MmL$
(6) $((4.1) \Leftrightarrow (Ue))$ *iff exactly one of:* $RrM, RmR, RmM, MrR, MrM, MmR$
(7) $((4.1) \Leftrightarrow (U1))$ *iff exactly one of:* $LrM, LmR, R\ell M, RmL, M\ell R, MrL$.

Case (7) gives us 288 solutions of Problem 2.1 but not all of them are new.

Acknowledgement. Partially supported through 'Algebra, Analysis and Applications' – a joint project of Serbian and Macedonian Academies of Sciences and Arts.

References

1. V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Nauka, Moscow, 1967. [in Russian]
2. V. D. Belousov, *Configurations in Algebraic Nets*, Stiintsa, Kishinev, 1979. [in Russian]
3. O. Chein, H. O. Pflugfelder, J. D. H. Smith, *Quasigroups and Loops: Theory and Applications*, Sigma Ser. Pure Math. **8** (1990), ISBN 3-88538-008-0.
4. T. Evans, *Variety of loops and quasigroups*, Chapter 1 of [**3**], 1990.
5. J. Fempl-Mađarević, A. Krapež, *Perfect quasigroup identities*, manuscript, 2018.
6. R. A. Fisher, *The design of experiments*, 8$^{\text{th}}$ edition, Oliver & Boyd, Edinburgh, 1966.
7. C. Kościelny, *A method for constructing quasigroup-based stream-ciphers*, Appl. Math. Comput. Sci. **6** (1996), 109–121.
8. A. Krapež, *An application of quasigroups in cryptology*, Math. Maced. **8** (2010), 47–52.
9. A. Krapež, B. Šešelja, A. Tepavčević, *Solving linear equations by fuzzy quasigroups techniques*, to appear in Inf. Sci., (2019); DOI 10.1016/j.ins.2019.03.073.
10. A. Krapež, V. A. Shcherbacov, *Quasigroups, units and Belousov's problem # 18*, Armen. J. Math. 2019, to appear.
11. P. Krömer, J. Platoš, J. Nowakova, V. Snasel, *An acceleration of quasigroup operations by residue arithmetic*, Concurrency Comput. Pract. Exp. **2017** (2017), DOI: 10.1002/cpe
12. S. Markovski, *Quasigroup string processing and applications in cryptography*, in: *Proc. 1st. Inter. Conf. Mathematics and Informatics for industry, MII 2003, 14–16 April*, Thessaloniki, 2003, 278–290.
13. S. Markovski, *Design of crypto primitives based on quasigroups*, Quasigroups Relat. Syst. **23** 2015, 41–90.
14. R. Moufang. *Zur Struktur von Alternativkörpern*, Math. Ann. **110**(1) (1935), 416–430, doi: 10.1007/BF01448037.
15. H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.
16. V. Shcherbacov, *Elements of Quasigroup Theory and Applications*, Chapman & Hall/CRC Monographs and Research Notes in Mathematics, Boca Raton, 2017.
17. J. D. H. Smith, *An introduction to Quasigroups and Their Representation*, Chapman and Hall/CRC Studies in Advanced Mathematics, London, 2007.
18. A. Ungar, *Beyond the Einstein Addition Law and its Gyroskopic Thomas Precession – The Theory of Gyrogroups and Gyrovector Spaces*, Kluwer Academic Publishers, 2001.

Mathematical Institute of the SASA
Belgrade Serbia
sasa@mi.sanu.ac.rs

(Received 06 11 2017)