Units in quasigroups

Aleksandar Krapež
(with J. Fempl–Madjarević and V. A. Shcherbacov)

Mathematical Institute of the SASA
Belgrade, Serbia

AAA 94
NSAC 2017
Novi Sad, June 14–18, 2017
Dedicated to B. Šešelja, colleague and friend
Quasigroups: the first definition

A \textit{quasigroup} is a groupoid \((Q; \cdot)\) such that linear equations:

\[ a \cdot x = b \quad \quad \quad y \cdot a = b \]

are uniquely solvable for all \(a, b \in Q\).
Quasigroups: the second definition

**Quasigroups** are algebras \((Q; \cdot, /, \backslash)\) satisfying:

\[
\begin{align*}
    xy / y &= x & x \backslash xy &= y \\
    (x / y)y &= x & x(x \backslash y) &= y
\end{align*}
\]
Quasigroups

Sometimes they are called

- equasigroups
- primitive quasigroups
- 3–quasigroups

A class of all 3–quasigroups is a variety.
The easiest way to 'understand' quasigroups is:

Quasigroups are 'not necessarily associative' groups. **(WRONG!)**

Groups are associative quasigroups. **(right)**
Another 'deficiency' of quasigroups is that they do not necessarily have a *unit*.

unit = our name for *neutral element* or *identity element*.
# Units

<table>
<thead>
<tr>
<th>unit</th>
<th>symbol</th>
<th>id 1</th>
<th>id 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>(Q)</td>
<td>$x = x$</td>
<td>$x = x$</td>
</tr>
<tr>
<td>left</td>
<td>(eQ)</td>
<td>$ex = x$</td>
<td>$x/x = y/y$</td>
</tr>
<tr>
<td>right</td>
<td>(Qe)</td>
<td>$xe = x$</td>
<td>$x \setminus x = y \setminus y$</td>
</tr>
<tr>
<td>middle</td>
<td>(U)</td>
<td>$xx = e$</td>
<td>$xx = yy$</td>
</tr>
<tr>
<td>$\ell + r$</td>
<td>(1)</td>
<td>$ex = x, xe = x$</td>
<td>$x/x = y \setminus y$</td>
</tr>
<tr>
<td>$\ell + m$</td>
<td>(eU)</td>
<td>$ex = x, xx = e$</td>
<td>$x/x = yy$</td>
</tr>
<tr>
<td>$r + m$</td>
<td>(Ue)</td>
<td>$xe = x, xx = e$</td>
<td>$x \setminus x = yy$</td>
</tr>
<tr>
<td>$\ell + r + m$</td>
<td>(U1)</td>
<td>$ex = x, xe = x, xx = e$</td>
<td>$x/x = y \setminus y = zz$</td>
</tr>
</tbody>
</table>
Units

1st family – Identities similar to weak associativity
2nd family – closed identities
3rd family – derivative autotopies
Belousov’s problem

Problem (Belousov (1969))

*How to recognize identities which force quasigroups satisfying them to be loops?*
Examples

Associativity:

\[ x \cdot yz = xy \cdot z \]

which defines groups.

Four Moufang identities:

\[ z(x \cdot zy) = (zx \cdot z)y \]
\[ x(z \cdot yz) = (xz \cdot y)z \]
\[ zx \cdot yz = (z \cdot xy)z \]
\[ zx \cdot yz = z(xy \cdot z) \]

which define Moufang loops (Kunen (1996), using Prover).
Problem (Krapež, Shcherbacov)

How to recognize identities which force quasigroups satisfying them to have \{left, right, middle\} unit?
Examples

Left Bol identity:
\[ x(y \cdot xz) = (x \cdot yx)z \]
implies existence of a right unit.

Right Bol identity:
\[ x(yz \cdot y) = (xy \cdot z)y \]
implies existence of a left unit.
J. D. H. Smith (2007) proved that the identity of weak associativity:

\[ x(y/y) \cdot z = x \cdot (y/y)z \]

implies (1).
Theorem (Krapež, Shcherbacov)

- Identity \( x(y\setminus y) \cdot z = x \cdot (y\setminus y)z \) implies (1).
- Identity \( (x\setminus yy)\setminus z = x\setminus(yy\setminus z) \) implies (eU).
- Identity \( (x\setminus(y/y))\setminus z = x\setminus((y/y)\setminus z) \) implies (eU).
- Identity \( (x\setminus yy)/z = x/(yy/z) \) implies (Ue).
- Identity \( (x/(y\setminus y))/z = x/((y\setminus y)/z) \) implies (Ue).
Theorem (Krapež)

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

$$xA((yBy)Cz) = (xD^{-1}(yDy))Az \quad (WA)$$

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

- $e$ is the middle unit for $B$,
- $e$ is the left unit for $C$,
- $i$ is the middle unit for $D$.

The converse also holds.
Parastrophes

Operations $\cdot, *, /, \backslash, \backslash\backslash, \backslash\backslash\backslash$ are parastrophes of $\cdot$ (and of each other):

$x \cdot y = z$ iff $x \backslash z = y$ iff $z / y = x$ iff

$y \ast x = z$ iff $z \backslash\backslash x = y$ iff $y \backslash\backslash\backslash z = x$

There are six parastrophes for any quasigroup.
We are interested in (WA) when $A, B, C, D$ are parastrophes of a quasigroup $\cdot$. Then:

- All four operations are quasigroups;
- The units $e$ and $i$ are equal;
- $e = i$ is some kind of unit for $\cdot$.

On the contrary,
the choice of $A$ does not impose any restriction on $\cdot$. 
Let us define two partitions on $\Pi = \{\cdot, *, /, \backslash, //, \backslash/\}$:

First: $L = \{/ , //\}$, $R = \{\backslash, \backslash/\}$, $M = \{\cdot, *\}$

Second: $\ell = \{\cdot, \backslash\}$, $r = \{*, //\}$, $m = \{/, \backslash/\}$. 
Classification of $WA$–identities

Theorem (Krapež)

$\text{(WA)} \iff \text{(eQ)}$ iff $L \ll L$

iff $A \in \Pi, B \in L, C \in \ell, D \in L$.

There are 48 $WA$–identities equivalent to $(eQ)$.
Example

Let $A$ be $\backslash$, $B$ be $\sslash$, $C$ be $\cdot$ and $D$ be $/$.
Then $D^{-1}$ is $\sslash$ and the appropriate $WA$–identity is:

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

Translating to the language of quasigroups, we get that all quasigroups satisfying:

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

have left unit.
Classification of WA–identities

Analogously:

There are 48 WA–identities equivalent to (Qe).
There are 48 WA–identities equivalent to (U).
There are 288 WA–identities equivalent to (1).
There are 288 WA–identities equivalent to (eU).
There are 288 WA–identities equivalent to (Ue).
There are 288 WA–identities equivalent to (U1).
Closed identities

Definition

Let \( s = t \) be a quasigroup identity. A subterm \( u \) of \( s(t) \) is closed if

- \( u \) is a variable, or
- for every variable \( x \) from \( s = t \),
  \( u \) either contains all appearances of \( x \) or none.

Identity \( s = t \) is closed if every subterm \( u \) of \( s(t) \) is closed.
Examples

1. Trivial identity $x = x$ is closed.

2. The identity $xy = xy$ is trivial, but not closed.

3. Collapsing identities $x = y$ and $x = e$ are closed.

4. The identity $x = y \cdot yy$ is collapsing but not closed.
Basic terms

A quasigroup term $b$ is \textit{basic} if:

- $b$ is a variable ($b$ is \textit{linear}); or
- $b = x \circ x$ for some variable $x$
  and some $\circ \in \{\cdot, /, \backslash\}$ ($b$ is \textit{quadratic}).
Representation

Theorem (Fempl–Madjarević, Krapež)

Let $s = t$ be nontrivial closed quasigroup identity. Then there are linear terms $L_1[x_1, \ldots, x_k], L_2[x_{k+1}, \ldots, x_n]$ such that

$s = L_1[b_1, \ldots, b_k]$
$t = L_2[b_{k+1}, \ldots, b_n]$

where $b_i$ ($1 \leq i \leq n$) are basic terms and

$$s = t \iff \bigwedge_{i=1}^{n} (b_i = e).$$

If at least one of $b_i$ is linear, then $s = t$ is collapsing.

Otherwise, $s = t$ is equivalent to the one of:

$(eQ), (Qe), (U), (1), (eU), (Ue), (U1)$. 
Translations

Definition

For a given quasigroup \((Q; \cdot, /, \backslash)\), translations are:

\[
\begin{align*}
L_a(x) &= a \cdot x & L_a^{-1}(x) &= a \backslash x \\
R_a(x) &= x \cdot a & R_a^{-1}(x) &= x / a \\
P_a(x) &= x \backslash a & P_a^{-1}(x) &= a / x
\end{align*}
\]

It is convenient to have numerical values for translations:

<table>
<thead>
<tr>
<th>(\varepsilon)</th>
<th>(L)</th>
<th>(R)</th>
<th>(P)</th>
<th>(P^{-1})</th>
<th>(R^{-1})</th>
<th>(L^{-1})</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
We shorten:

\[ D(x, y) = \gamma^{-1} A(\alpha x, \beta y) \]

to:

\[ D = A(\alpha, \beta, \gamma). \]
Belousov’s derivatives

\[ A_a = A(L_a, \varepsilon, L_a) \]  
(Right derivative)

\[ aA = A(\varepsilon, R_a, R_a) \]  
(Left derivative)

\[ A_a = A(P_a, P_a, \varepsilon) \]  
(Middle derivative)
Derivatives

\[ D = A(\alpha, \beta, \gamma) \text{ is derivative if:} \]
- \( \alpha, \beta, \gamma \) are bijections
- one of them is \( \varepsilon \).

\[ D_a = A(\alpha, \beta, \gamma) \text{ is inner derivative (relative to } a \in Q) \text{ if:} \]
- the one of \( \alpha, \beta, \gamma \) is \( \varepsilon \)
- the other two are translations (by \( a \)).
Problem

$D_a = A$ implies the existence of an autotopy of $A$.
Does it imply the existence of some unit?
For every identity $D_a = A$ we have a three digit number $pqr$ (where one of $p, q, r$ is 0 (which stands for $\varepsilon$) and the other two are numbers between 1 and 6 (and they stand for appropriate translations by $a$). If one of $p, q, r$ is $n$ it means that it stands for all numbers from 1 to 6.

For example, the identity $A_a = A$ is represented by the number 101.
Results

Theorem (Krapež, Shcherbacov)

$$pqr \Rightarrow (eQ) \text{ for } pqr \in \{ n01, n06, n10, n60, 102, 105, 130, 140, 602, 605, 630, 640 \}.$$
Analogously:

\[ pqr \Rightarrow (Qe) \text{ for } pqr \in \{0n2, 0n5, 2n0, 5n0, 021, 026, 051, 056, 320, 350, 420, 450\}. \]

\[ pqr \Rightarrow (U) \text{ for } pqr \in \{03n, 04n, 30n, 40n, 013, 014, 063, 064, 203, 204, 503, 504\}. \]

\[ pqr \Rightarrow (1) \text{ for } pqr \in \{210, 260, 510, 560\}. \]

\[ pqr \Rightarrow (eU) \text{ for } pqr \in \{301, 306, 401, 406\}. \]

\[ pqr \Rightarrow (Ue) \text{ for } pqr \in \{032, 035, 042, 045\}. \]

\[ pqr \Rightarrow (U1) \text{ for no } pqr. \]