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

Dedication

Dedicated to B. Šešelja,

colleague and friend

Quasigroups

Quasigroups: the first definition

A *quasigroup* is a groupoid $(Q; \cdot)$ such that linear equations:

$$a \cdot x = b \qquad\qquad y \cdot a = b$$

are uniquely solvable for all $a, b \in Q$.

Quasigroups

Quasigroups: the second definition

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

$$\begin{aligned} xy/y &= x & \qquad x\backslash xy &= y \\ (x/y)y &= x & \qquad x(x\backslash y) &= y \end{aligned}$$

Quasigroups

Sometimes they are called

- equasigroups
- primitive quasigroups
- 3–quasigroups

A class of all 3–quasigroups is a variety.

Quasigroups

The easiest way to 'understand' quasigroups is:

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

Groups are associative quasigroups. **(right)**

Quasigroups

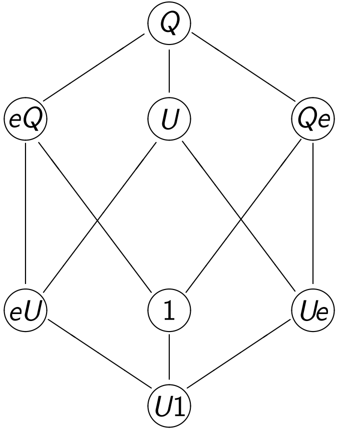
Another 'deficiency' of quasigroups
is that they do not necessarily have a *unit*.

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

Units

unit	symbol	id 1	id 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	(1)	$ex = x, xe = x$	$x/x = y\backslash y$
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	$x/x = y\backslash y = zz$

Units



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).

Another problem

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.

Weak associativity

J. D. H. Smith (2007) proved that the identity of weak associativity:

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

implies (1).

Identites similar to weak associativity

Theorem (Krapež, Shcherbacov)

- Identity $x(y\backslash y) \cdot z = x \cdot (y\backslash y)z$ implies (1).

- Identity $(x\backslash yy)\backslash z = x\backslash(yy\backslash z)$ implies (eU).
- Identity $(x\backslash(y/y))\backslash z = x\backslash((y/y)\backslash z)$ implies (eU).

- Identity $(x/yy)/z = x/(yy/z)$ implies (Ue).
- Identity $(x/(y\backslash y))/z = x/((y\backslash y)/z)$ implies (Ue).

Weak associativity – general form

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:

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

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

$$\begin{array}{llllll} x \cdot y = z & \text{iff} & x \backslash z = y & \text{iff} & z / y = x & \text{iff} \\ y * x = z & \text{iff} & z \backslash\!\!\backslash x = y & \text{iff} & y /\!\!/ z = x & \end{array}$$

There are six parastrophes for any quasigroup.

Weak associativity for parastrophes

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 $\cdot$.

Partitions of Π

Let us define two partitions on $\Pi = \{\cdot, *, /, \backslash, /\!\!/, \backslash\!\!\backslash\}$:

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

Second: $\ell = \{\cdot, \backslash\}, r = \{*, /\!\!/\}, m = \{/, \backslash\!\!\backslash\}$.

Classification of *WA*–identities

Theorem (Krapež)

(WA) $\Leftrightarrow$ *(eQ) iff* $L\ell L$

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

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

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 *basic* if:

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

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

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:

$$
\begin{aligned}
L_a(x) &= a\cdot x & \quad L_a^{-1}(x) &= a\backslash x\\
R_a(x) &= x\cdot a & \quad R_a^{-1}(x) &= x/a\\
P_a(x) &= x\backslash a & \quad P_a^{-1}(x) &= a/x
\end{aligned}
$$

It is convenient to have numerical values for translations:

	ε	L	R	P	P^{-1}	R^{-1}	L^{-1}
value	0	1	2	3	4	5	6

Definition

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)

$\underset{a}{A} = A(P_a, P_a, \varepsilon)$ (Middle derivative)

Derivatives

$D = A(\alpha, \beta, \gamma)$ is *derivative* if:

- α, β, γ are bijections
- one of them is ε.

$D_a = A(\alpha, \beta, \gamma)$ is *inner derivative (relative to $a \in Q$)* if:

- the one of α, β, γ is ε
- the other two are translations (by a).

Problem

Problem

$D_a = A$ implies the existence of an autotopy of A.
Does it imply the existence of some unit?

Numbers for identities

For every identity $D_a = A$ we have a three digit number pqr (where one of p, q, r is 0 (which stands for ε) 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*) *for*
$pqr \in \{n01, n06, n10, n60, 102, 105, 130, 140, 602, 605, 630, 640\}$.

Results

Analogously:

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

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

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

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

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

$pqr \Rightarrow (U1)$ for no pqr.