Defining Quasigroups

Jonathan D.H. Smith

Department of Mathematics,
Iowa State University,
Ames, Iowa 50011-2064, U.S.A.

email: jdhsmith@math.iastate.edu

http://orion.math.iastate.edu/jdhsmith/homepage.html
- Combinatorial quasigroups
- Equational quasigroups
- Reflexion-inversion spaces
- 5 examples of reflexion-inversion spaces
- Hyperquasigroups
- 5 examples of hyperquasigroups
- From hyperquasigroups to quasigroups
- $n$-quasigroups
COMBINATORIAL QUASIGROUPS

(Combinatorial) quasigroup \((Q, \cdot)\):

In \[x \cdot y = z\]
specifying two of

\[x, y, z\]
specifies the third uniquely.

For \(q \in Q\), **left multiplication**

\[L(q) : Q \rightarrow Q; x \mapsto qx\] bijects.

**Right multiplication**

\[R(q) : Q \rightarrow Q; x \mapsto xq\] bijects.
EQUATIONAL QUASIGROUPS

(Equational) quasigroup $(Q, \cdot, /, \backslash)$:

(IL) $y \backslash (y \cdot x) = x$; --- injectivity of $L(y)$

(IR) $x = (x \cdot y)/y$; --- injectivity of $R(y)$

(SL) $y \cdot (y\backslash x) = x$; --- surjectivity of $L(y)$

(SR) $x = (x/y) \cdot y$; --- surjectivity of $R(y)$

The quasigroups $(Q, \cdot)$, $(Q, /)$, $(Q, \backslash)$ and their opposites are the conjugates (or “parastrophes”) of $(Q, \cdot)$. 
REFLEXION - INVERSION SPACES

Reflexion-inversion space \((G, \sigma, \tau)\):

Set \(G\),

with involutary reflexion

\(\sigma : G \rightarrow G; g \mapsto \sigma g\),

and involutary inversion

\(\tau : G \rightarrow G; g \mapsto \tau g\).

Involutary means

\(\sigma\sigma g = g\) and \(\tau\tau g = g\)

for each point \(g\) of the space \(G\).
equivalently . . .

for the **infinite dihedral group**

\[ D_\infty = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = 1 \rangle \]

— set of words in \( \sigma \) and \( \tau \) without repeats in adjacent letters, multiplication by juxtaposition and cancellation,

e.g. \( \tau \sigma \cdot \sigma \tau \sigma \tau = \sigma \tau \),

inversion reverses words —

reflexion-inversion spaces \( G \)

are left \( D_\infty \)-sets,

with chosen involutions \( \sigma \) and \( \tau \).
EXAMPLE 1: FIELDS

For field $F$, take $G = F \setminus \{0, 1\},$
reflexion $\sigma : G \rightarrow G; g \mapsto 1 - g,$
inversion $\tau : G \rightarrow G; g \mapsto g^{-1}.$

Inversion is always true inversion.

If $F$ is not of characteristic 2, reflexion is true reflexion in the point $\frac{1}{2}$. 
EXAMPLE 2: GROUPS

Group $G$ with involutions $\sigma$, $\tau$
forms a reflexion-inversion space
in which reflexion is left multiplication by $\sigma$,
and inversion is left multiplication by $\tau$. 
EXAMPLE 3: THE SPACE $T^2 \times \mathbb{R}^2$

Let $\mathbb{C}/2\pi i\mathbb{Z}$ be the quotient of $\mathbb{C}$

by the equivalence relation $\{(z, z') \in \mathbb{C}^2 \mid z - z' \in 2\pi i\mathbb{Z}\}$.

Representatives live in the fundamental domain

$\{x + iy \in \mathbb{C} \mid x \in \mathbb{R}, y \in [0, 2\pi) \subset \mathbb{R}\}$.

Take $G = (\mathbb{C}/2\pi i\mathbb{Z})^2$,

with $\sigma : G \to G; (a, b) \mapsto (b, a)$

and $\tau : G \to G; (a, b) \mapsto (i\pi + a - b, -b)$. 
EXAMPLE 4: THE EVEN GRID

Let $n$ be an even number, and let $G = (\mathbb{Z}/n\mathbb{Z})^2$.

Define $\sigma : G \to G; (a, b) \mapsto (b, a)$
and $\tau : G \to G; (a, b) \mapsto (a - b + n/2, -b)$.
EXAMPLE 5: ABELIAN GROUPS

Let $A$ be an abelian group, and let $G = A^2$.

Define $\sigma : G \to G; (a, b) \mapsto (b, a)$

and $\tau : G \to G; (a, b) \mapsto (a - b, -b)$.

Here, reflexion and inversion are linear.
HYPERQUASIGROUPS

A hyperquasigroup \((Q, G)\)

consists of a set \(Q\) and a reflexion-inversion space \(G\),
together with a binary action
\[
Q^2 \times G \rightarrow Q; (x, y, g) \mapsto x y g
\]
satisfying the hypercommutative law
\[
xy \sigma g = yx g
\]
and the hypercancellation law
\[
x (xy g) \tau g = y.
\]
HYPERCANCELLATIVITY

PROPOSITION: For a point $g$ in the space $G$ of a hyperquasigroup $(Q, G)$, define $\hat{g} : Q^2 \to Q^2; (x, y) \mapsto (x, xy \underline{g})$.

Then in the monoid of all self-maps on $Q^2$, the element $\hat{\tau}g$ is the inverse of $\hat{g}$.

Proof: $(x, y) \xrightarrow{\hat{g}} (x, xy \underline{g}) \xrightarrow{\hat{\tau}g} (x, x (xy \underline{g}) \underline{\tau g}) = (x, y)$

and $(x, y) \xrightarrow{\hat{\tau}g} (x, xy \underline{\tau g}) \xrightarrow{\hat{g}} (x, x (xy \underline{\tau g}) \underline{g}) = (x, y)$. 
EXAMPLE 1: FIELDS

Field $F$, $G = F \setminus \{0, 1\}$, $\sigma : G \to G$; $g \mapsto 1 - g$, and $\tau : G \to G$; $g \mapsto g^{-1}$. Vector space $Q$ over $F$ gives hyperquasigroup $(Q, G)$:

$xyg = x(1 - g) + yg$ for $x, y$ in $Q$ and $g$ in $G$.

Hypercommutativity:

$xy\sigma g = x(1 - (1 - g)) + y(1 - g) = yxg$

Hypercancellativity:

$x(xyg)\tau g = x(1 - g^{-1}) + (x(1 - g) + yg)g^{-1} = y$
EXAMPLE 2: (QUASI)GROUPS

Group $G = S_3$, transpositions $\sigma = (1\ 2)$ and $\tau = (2\ 3)$.

For equational quasigroup $(Q, \cdot, /, \\backslash)$, 

$(Q, G)$ becomes a hyperquasigroup with 

\[
xy_1 = x \cdot y, \quad xy\sigma\tau\sigma = x/y, \quad xy\tau = x\backslash y, \\
xy\sigma = y \cdot x, \quad xy\tau\sigma = y/x, \quad xy\sigma\tau = y\backslash x.
\]
### EXAMPLES 3 – 5

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma : (a, b) \mapsto (b, a)$</td>
<td>$xy(a, b) = xe^a + ye^b$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3</strong> $G = (\mathbb{C}/2\pi i\mathbb{Z})^2$,</td>
<td>Complex vector space $Q$</td>
</tr>
<tr>
<td>$\tau : (a, b) \mapsto (i\pi + a - b, -b)$</td>
<td></td>
</tr>
<tr>
<td><strong>4</strong> $G = (\mathbb{Z}/n\mathbb{Z})^2$, even $n$,</td>
<td>Unital ring $R$, root $e$ of $X^{n/2} + 1$ in $R$,</td>
</tr>
<tr>
<td>$\tau : (a, b) \mapsto (a - b + n/2, -b)$</td>
<td>unital right $R$-module $Q$</td>
</tr>
<tr>
<td><strong>5</strong> $G = \mathbb{Z}^2$,</td>
<td>Invertible $e$ in ring $R$ of characteristic 2,</td>
</tr>
<tr>
<td>$\tau : (a, b) \mapsto (a - b, -b)$</td>
<td>unital right $R$-module $Q$</td>
</tr>
</tbody>
</table>
THEOREM: Let \((Q, G)\) be a hyperquasigroup.

Then for each point \(g\) in the space \(G\),

have equational quasigroup \((Q, σg, στg, τσg)\).

COROLLARY: Let \((Q, G)\) be a hyperquasigroup.

Then for each point \(g\) in the space \(G\),

have combinatorial quasigroup \((Q, g)\).
PROOF OF THE THEOREM

(IL) for \((Q, \sigma g, \sigma \tau g, \tau \sigma g)\) is \(y = x (xy \sigma g) \tau \sigma g\),
which is hypercancellativity with \(\sigma g\) replacing \(g\).

(IR) is \(y = (yx \sigma g) x \sigma \tau g\), which follows from
the hypercancellativity \(y = x (xy \sigma g) \tau g\), using hypercommutativity.

(SL) is \(y = x (xy \tau \sigma g) \sigma g\),
which is hypercancellativity with \(\sigma g\) replacing \(g\).

(SR) is \(y = (yx \sigma \tau g) x \sigma g\), a rewrite via hypercommutativity
of hypercancellativity \(y = x (xy \tau g) g\) (with \(\tau g\) replacing \(g\)).
EXAMPLES

EXAMPLE 1: For a finite field $F$ of order $q$,

$$G = F \setminus \{0, 1\}, \text{ and } Q = F,$$

corollary gives $q - 2$ mutually orthogonal idempotent quasigroups.

EXAMPLE 2: For a quasigroup $(Q, \cdot)$,

and $G = S_3$,

corollary gives the full set of 6 conjugates of $(Q, \cdot)$.
$S_3$-ACTIONS

**PROPOSITION:** Let $(Q, G)$ be a hyperquasigroup. Then for all $x, y$ in $Q$ and $g$ in $G$,

$$xy \sigma \tau \sigma g = xy \tau \sigma \tau g.$$ 

**THEOREM:** Each hyperquasigroup $(Q, G)$ yields an algebra structure $(Q, G')$ consisting of the union

$$G = \bigcup_{g \in G} S_3 g$$

does not mutually disjoint sets of conjugate quasigroup operations.
$n$-ARY QUASIGROUPS

Binary hyperquasigroup:

\[ x_2 x_1 \sigma g = x_1 x_2 g, \quad x_1 (x_1 x_2 g) \tau g = x_2 \]

Ternary hyperquasigroup:

\[ x_2 x_3 x_1 \sigma g = x_1 x_2 x_3 g, \quad x_1 x_2 (x_1 x_2 x_3 g) \tau g = x_3 \]

$n$-ary hyperquasigroup:

\[ x_2 \ldots x_n x_1 \sigma g = x_1 \ldots x_n g, \quad x_1 \ldots x_{n-1} (x_1 \ldots x_n g) \tau g = x_n \]

Unary hyperquasigroup:

\[ x_1 \sigma g = x_1 g, \quad (x_1 g) \tau g = x_1 \]
CORRESPONDING SPACES

Unary case:
Cyclic group \( \langle \sigma, \tau \mid \sigma^1 = \tau^2 = 1 \rangle \)

Binary case:
Infinite dihedral group \( \langle \sigma, \tau \mid \sigma^2 = \tau^2 = 1 \rangle \)

Ternary case:
Modular group \( \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1 \rangle \)