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 $\boxed{x \cdot y = z}$

specifying two of

x, y, z

specifies the third uniquely.

For $q \in Q$, **left multiplication**

$L(q) : Q \to Q; x \mapsto qx$ bijects.

Right multiplication

$R(q) : Q \to Q; x \mapsto xq$ 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, σ, τ):

Set G,

with involutary **reflexion**

$\sigma : G \to G; g \mapsto \sigma g$,

and involutary **inversion**

$\tau : G \to G; g \mapsto \tau g$.

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 σ and τ 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_∞-sets,

with chosen involutions σ and τ.

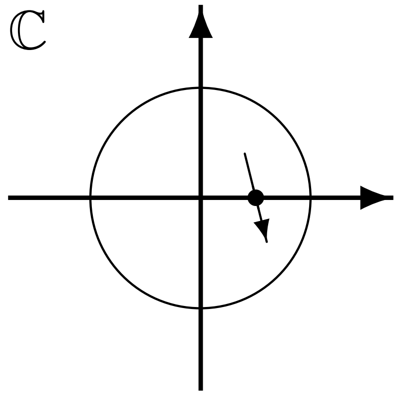
EXAMPLE 1: FIELDS

For field F, take $G = F \setminus \{0, 1\}$,

reflexion $\sigma : G \longrightarrow G; g \mapsto 1 - g$,

inversion $\tau : G \longrightarrow G; g \mapsto g^{-1}$.

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 σ, τ

forms a reflexion-inversion space

in which reflexion is left multiplication by σ,

and inversion is left multiplication by τ.

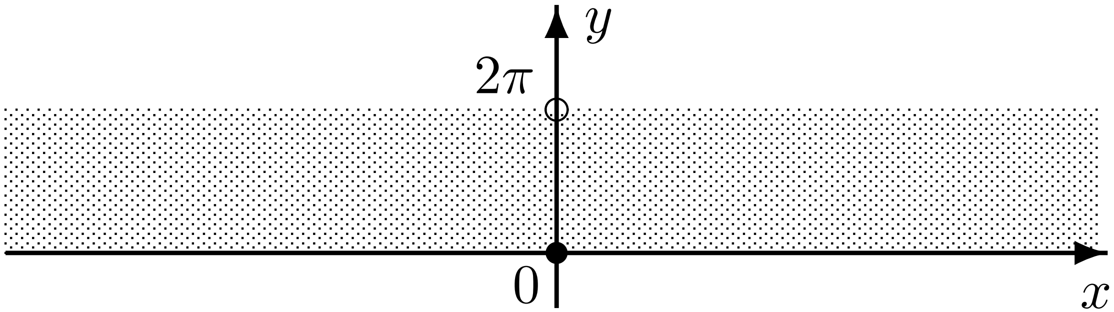
EXAMPLE 3: THE SPACE $T^2 \times \mathbb{R}^2$

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

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



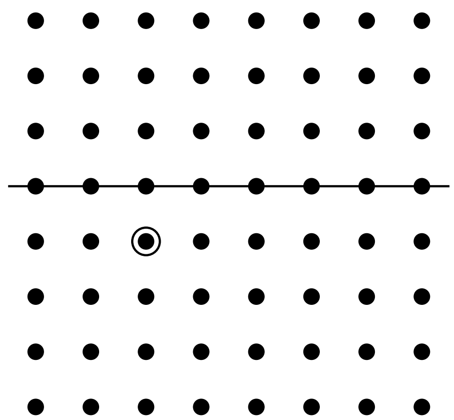
Take $G = (\mathbb{C}/2\pi i\mathbb{Z})^2$,

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 $\tau : G \to G; (a,b) \mapsto \big(a - b + n/2, -b\big)$.

EXAMPLE 5: ABELIAN GROUPS

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

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

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

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

$$Q^2 \times G \to Q; (x, y, g) \mapsto xy\,\underline{g}$$

satisfying the **hypercommutative law**

$$xy\,\underline{\sigma g} = yx\,\underline{g}$$

and the **hypercancellation law**

$$x\,(xy\,\underline{g}\,)\,\underline{\tau g} = y.$$

HYPERCANCELLATIVITY

PROPOSITION: For a point g in the space G of a hyperquasigroup (Q, G),

define $\widehat{g} : Q^2 \to Q^2; (x, y) \mapsto (x, xy\,\underline{g})$.

Then in the monoid of all self-maps on Q^2,

the element $\widehat{\tau g}$ is the inverse of $\widehat{g}$.

Proof: $(x, y) \overset{\widehat{g}}{\mapsto} (x, xy\,\underline{g}) \overset{\widehat{\tau g}}{\mapsto} \big(x, x\,(xy\,\underline{g}\,)\,\underline{\tau g}\,\big) = (x, y)$

and $(x, y) \overset{\widehat{\tau g}}{\mapsto} (x, xy\,\underline{\tau g}) \overset{\widehat{g}}{\mapsto} \big(x, x\,(xy\,\underline{\tau g}\,)\,\underline{g}\,\big) = (x, y)$.

EXAMPLE 1: FIELDS

Field F,

$G = F \smallsetminus \{0, 1\}$,

$\sigma : G \to G$;

$g \mapsto 1 - g$, and

$\tau : G \to G$;

$g \mapsto g^{-1}$.

Vector space Q over F gives hyperquasigroup (Q, G):

$$xy\,\underline{g} = x(1-g) + yg$$

for x, y in Q and g in G.

Hypercommutativity:

$$xy\,\underline{\sigma g} = x\big(1 - (1-g)\big) + y(1-g) = yx\,\underline{g}$$

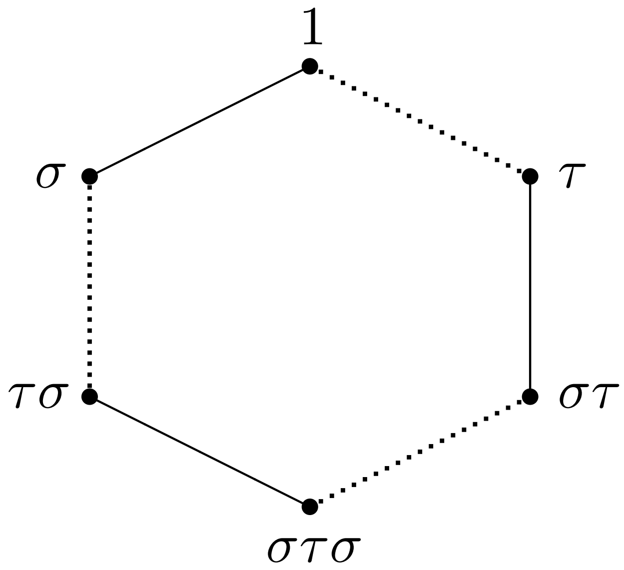
Hypercancellativity:

$$x\,(xy\,\underline{g}\,)\,\underline{\tau g}$$

$$= x(1-g^{-1}) + \big(x(1-g) + yg\big)g^{-1} = y$$

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

$$xy\,\underline{1} = x \cdot y\,, \quad xy\,\underline{\sigma\tau\sigma} = x/y\,, \quad xy\,\underline{\tau} = x\backslash y\,,$$

$$xy\,\underline{\sigma} = y \cdot x\,, \quad xy\,\underline{\tau\sigma} = y/x\,, \quad xy\,\underline{\sigma\tau} = y\backslash x\,.$$

EXAMPLES 3 – 5

$\sigma : (a,b) \mapsto (b,a)$	$xy\,\underline{(a,b)} = xe^a + ye^b$
(3) $G = (\mathbb{C}/2\pi i\mathbb{Z})^2$, $\tau : (a,b) \mapsto (i\pi + a - b, -b)$	Complex vector space Q
(4) $G = (\mathbb{Z}/n\mathbb{Z})^2$, even n, $\tau : (a,b) \mapsto (a - b + n/2, -b)$	Unital ring R, root e of $X^{n/2} + 1$ in R, unital right R-module Q
(5) $G = \mathbb{Z}^2$, $\tau : (a,b) \mapsto (a - b, -b)$	Invertible e in ring R of characteristic 2, unital right R-module Q

FROM HYPERQUASIGROUPS TO QUASIGROUPS

THEOREM: Let (Q, G) be a hyperquasigroup.

Then for each point g in the space G,

have equational quasigroup $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$.

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

Then for each point g in the space G,

have combinatorial quasigroup $(Q, \underline{g})$.

PROOF OF THE THEOREM

(IL) for $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$ is $y = x\,(xy\,\underline{\sigma g}\,)\,\underline{\tau\sigma g}$,

which is hypercancellativity with σg replacing g.

(IR) is $y = (yx\,\underline{\sigma g}\,)\,x\,\underline{\sigma\tau g}$, which follows from

the hypercancellativity $y = x\,(xy\,\underline{g}\,)\,\underline{\tau g}$, using hypercommutativity.

(SL) is $y = x\,(xy\,\underline{\tau\sigma g}\,)\,\underline{\sigma g}$,

which is hypercancellativity with σg replacing g.

(SR) is $y = (yx\,\underline{\sigma\tau g}\,)\,x\,\underline{\sigma g}$, a rewrite via hypercommutativity

of hypercancellativity $y = x\,(xy\,\underline{\tau g}\,)\,\underline{g}$ (with τg replacing g).

EXAMPLES

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

$G = F \setminus \{0, 1\}$, 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,

$xy\,\underline{\sigma\tau\sigma g} = xy\,\underline{\tau\sigma\tau g}$.

THEOREM: Each hyperquasigroup (Q, G)

yields an algebra structure $(Q, \underline{G})$ consisting of the union

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

of mutually disjoint sets of conjugate quasigroup operations.

n-ARY QUASIGROUPS

Binary hyperquasigroup:

$$x_2 x_1 \underline{\sigma g} = x_1 x_2 \underline{g}\ , \qquad x_1 \left(x_1 x_2 \underline{g}\right) \underline{\tau g} = x_2$$

Ternary hyperquasigroup:

$$x_2 x_3 x_1 \underline{\sigma g} = x_1 x_2 x_3 \underline{g}\ , \qquad x_1 x_2 \left(x_1 x_2 x_3 \underline{g}\right) \underline{\tau g} = x_3$$

n-ary hyperquasigroup:

$$x_2 \dots x_n x_1 \underline{\sigma g} = x_1 \dots x_n \underline{g}\ , \qquad x_1 \dots x_{n-1} \left(x_1 \dots x_n \underline{g}\right) \underline{\tau g} = x_n$$

Unary hyperquasigroup:

$$x_1 \underline{\sigma g} = x_1 \underline{g}\ , \qquad \left(x_1 \underline{g}\right) \underline{\tau g} = x_1$$

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 $\langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1 \rangle$