Discussiones Mathematicae
General Algebra and Applications 27(2007) 21–33

AXIOMATIZATION OF QUASIGROUPS

JONATHAN D.H. SMITH

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

e-mail: jdhsmith@math.iastate.edu
http://orion.math.iastate.edu/jdhsmith/

Abstract

Quasigroups were originally described combinatorially, in terms of existence and uniqueness conditions on the solutions to certain equations. Evans introduced a universal-algebraic characterization, as algebras with three binary operations satisfying four identities. Now, quasigroups are redefined as heterogeneous algebras, satisfying just two conditions respectively known as hypercommutativity and hypercancellativity.

Keywords: quasigroup, heterogeneous algebra, hyperidentity.

2000 Mathematics Subject Classification: Primary: 20N05; Secondary: 08A68.

1. INTRODUCTION

Quasigroups are one of the oldest topics in algebra and combinatorics, dating back at least to Euler [1]. Evans [2] showed how they could be defined in universal-algebraic fashion, using three binary operations and four identities. Nevertheless, this definition does not seem entirely satisfactory for such a fundamental object of mathematics, since it requires an explicit listing of the four apparently related identities. A new definition is presented in the current paper, using heterogeneous algebras known as *hyperquasigroups*. With this new definition, just two identities are needed: *hypercommutativity* and *hypercancellativity*.

The original combinatorial and equational definitions of quasigroups are recalled in Section 2. Section 3 introduces the higher level of a hyperquasigroup, a structure known as a *reflexion-inversion space*. Various examples of such spaces are discussed. Hyperquasigroups themselves are defined in Section 4. Section 5 then exhibits hyperquasigroups embodying each of the types of reflexion-inversion space presented in Section 3. In particular (Proposition 5.2), each quasigroup is part of a hyperquasigroup with the symmetric group S_3 on three symbols as the corresponding reflexion-inversion space. In the converse direction, Section 6 shows that each hyperquasigroup comprises a set equipped with disjoint sets of mutually conjugate quasigroup operations.

2. QUASIGROUPS

A quasigroup Q was first understood as a set equipped with a binary multiplication, denoted by $\cdot$ or mere juxtaposition, such that in the equation

$$x \cdot y = z \ ,$$

knowledge of any two of x, y, z specifies the third uniquely. To make a distinction with subsequent concepts, it is convenient to describe a quasigroup in this original sense as a *combinatorial quasigroup* $(Q, \cdot)$.

For each element q of a set Q with a binary multiplication denoted by $\cdot$ or juxtaposition, a *left multiplication* $L_Q(q)$ or

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

and *right multiplication* $R_Q(q)$ or

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

are obtained from the binary multiplication by the process of "Currying," the usual trick for reducing a function of two arguments (in this case the multiplication) to a parametrized family of functions of a single argument (compare [6]). If $(Q, \cdot)$ is a quasigroup, then the right and left multiplications are bijections of the underlying set Q. Indeed, the bijectivity of $L_Q(q)$ and $R_Q(q)$ for each element q of Q is equivalent with $(Q, \cdot)$ being a quasigroup.

Unfortunately, the combinatorial definition of a quasigroup is unsuitable for most algebraic purposes: A surjective multiplicative homomorphism $f : (Q, \cdot) \to (P, \cdot)$ whose domain is a combinatorial quasigroup $(Q, \cdot)$ may

have an image $(P, \cdot)$ which is not a combinatorial quasigroup (compare [6, Example I.2.2.1], for instance). To circumvent this problem, Evans [2] redefined quasigroups as *equational quasigroups*, sets $(Q, \cdot, /, \backslash)$ equipped with three binary operations of multiplication, *right division* / and *left division* $\backslash$, satisfying the identities:

(IL) $$x\backslash(x \cdot y) = y;$$

(IR) $$y = (y \cdot x)/x;$$

(SL) $$x \cdot (x\backslash y) = y;$$

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

Note that (IL), (IR) give the respective injectivity of the left and right multiplications, while (SL), (SR) give their surjectivity. Thus an equational quasigroup $(Q, \cdot, /, \backslash)$ yields a combinatorial quasigroup $(Q, \cdot)$. Conversely, a combinatorial quasigroup $(Q, \cdot)$ yields an equational quasigroup $(Q, \cdot, /, \backslash)$ with $x/y = xR(y)^{-1}$ and $x\backslash y = yL(x)^{-1}$.

In an equational quasigroup $(Q, \cdot, /, \backslash)$, the three equations

(2.1) $$x_1 \cdot x_2 = x_3\,, \qquad x_3/x_2 = x_1\,, \qquad x_1\backslash x_3 = x_2$$

are equivalent. Introducing the opposite operations

$$x \circ y = y \cdot x\,, \qquad x//y = y/x\,, \qquad x\backslash\backslash y = y\backslash x$$

on Q, the equations (2.1) are further equivalent to the equations

$$x_2 \circ x_1 = x_3\,, \qquad x_2//x_3 = x_1\,, \qquad x_3\backslash\backslash x_1 = x_2\,.$$

Thus each of

(2.2) $$(Q, \cdot), \quad (Q, /), \quad (Q, \backslash), \quad (Q, \circ), \quad (Q, //), \quad (Q, \backslash\backslash)$$

is a (combinatorial) quasigroup. In particular, note that the identities (IR) in $(Q, \backslash)$ and (IL) in (Q,/) yield the respective identities

(DL) $$x/(y\backslash x) = y\,,$$

(DR) $$y = (x/y)\backslash x$$

in the basic quasigroup divisions. The six quasigroups (2.2) are known as the *conjugates*, "parastrophes" [4, p. 43] [5] or "derived quasigroups" [3] of $(Q, \cdot)$.

3. Reflexion-inversion spaces

Hyperquasigroups, as defined in Section 4 below, consist of structure at three levels, amounting to a two-sorted algebra (compare Remarks 3.2 and 4.2). The second (higher-level) sort is given in this section as follows.

Definition 3.1. A *reflexion-inversion space* (G, σ, τ) is a set G equipped with two involutive actions, a *reflexion*

$$\sigma : G \to G; g \mapsto \sigma g \tag{3.1}$$

and an *inversion*

$$\tau : G \to G; g \mapsto \tau g\,. \tag{3.2}$$

The involutivity of the actions means that

$$\sigma\sigma g = g \quad \text{and} \quad \tau\tau g = g$$

for each point g of the reflexion-inversion space.

Remark 3.2. Let H be the free product of two copies $\langle\sigma\rangle$ and $\langle\tau\rangle$ of the group of order two. The underlying set of this group is the set of (possibly empty) words in the two-letter alphabet $\{\sigma, \tau\}$ having no consecutive letters repeated. The product is given by the juxtaposition of words, followed by cancellation of repeated pairs of letters. For example, $\tau\sigma \cdot \sigma\tau\sigma\tau = \sigma\tau$. Inversion in the group just reverses the words, for example $(\sigma\tau\sigma\tau)^{-1} = \tau\sigma\tau\sigma$. A reflexion-inversion space (G, σ, τ) as in Definition 3.1 may then be interpreted as a left H-set with actions specified by (3.1) and (3.2). It is nevertheless important to note that reflexion-inversion spaces are richer than H-sets, since their structure includes the choice of the specific involutions σ and τ.

The remainder of the section presents some typical examples of reflexion-inversion spaces that may form part of a hyperquasigroup structure. The first example serves to motivate the terminology of Definition 3.1.

Example 3.3. Let F be a field. Let G be the complement $F \setminus \{0, 1\}$ of the set $\{0, 1\}$ in F. Define

$$\sigma : G \to G; g \mapsto 1 - g$$

and

$$\tau : G \to G; g \mapsto g^{-1}\,.$$

Then (G, σ, τ) forms a reflexion-inversion space. Note that the abstract inversion τ is a literal inversion in this case. If F is the field of real or complex numbers, then the abstract reflexion σ is literal reflexion in the point $1/2$.

Example 3.4. Let G be a group containing two elements σ and τ with $\sigma^2 = \tau^2 = 1$. Then G forms a reflexion-inversion space in which the reflection and inversion are the respective left multiplications by σ and τ.

Example 3.5. Let $\mathbb{C}/2\pi i\mathbb{Z}$ denote the quotient of the set of complex numbers by the equivalence relation

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

It is also convenient to identify each equivalence class in the set $\mathbb{C}/2\pi i\mathbb{Z}$ with its unique representative element in the fundamental domain

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

Let $G = (\mathbb{C}/2\pi i\mathbb{Z})^2$. (Topologically, this space is the product $T^2 \times \mathbb{R}^2$ of a torus with a plane.) Define

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

and

$$\tau : G \to G; (a, b) \mapsto (i\pi + a - b, -b)\,.$$

Then G forms a reflexion-inversion space.

Example 3.6. 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

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

Then G forms a reflexion-inversion space.

Example 3.7. Let A be an abelian group, and let $G = A^2$. Define

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

and

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

Then G forms a reflexion-inversion space in which the reflexion and inversion are linear maps.

4. HYPERQUASIGROUPS

Basing on the concept of a reflexion-inversion space, the definition of a hyperquasigroup may now be given.

Definition 4.1. A *hyperquasigroup* (Q, G) is a pair consisting of a set Q and a reflexion-inversion space G, together with a binary operation

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

of G on Q, such that the *hypercommutative law*

$$xy\,\underline{\sigma g} = yx\,\underline{g} \tag{4.1}$$

and the *hypercancellation law*

$$x\,(xy\,\underline{g})\,\underline{\tau g} = y \tag{4.2}$$

are satisfied for all x, y in Q and g in G.

Remark 4.2. A hyperquasigroup may be interpreted as a two-sorted algebra (Q, G). Here G is a left H-set according to Remark 3.2. The set G then acts on Q as in Definition 4.1.

Remark 4.3. The prefix "hyper-" in Definition 4.1 reflects the substitution of variables at both levels in (4.1) and (4.2), comparable to the substitution at both the argument and the operator level in hyperidentities [7].

Hypercommutativity is straightforward. The meaning of hypercancellativity is given by the following.

Proposition 4.4. *Let (Q, G) be a hyperquasigroup. For each element g of G, define*

$$\widehat{g} : Q^2 \to Q^2; (x, y) \mapsto (x, xy\,\underline{g})\,. \tag{4.3}$$

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

Proof. For x, y in Q, one has

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

with the equality holding directly by the hypercancellativity (4.2). Similarly, one has

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

the equality here resulting from the hypercancellation equation (4.2) with g replaced by τg. Thus $\widehat{\tau g}$ is indeed the inverse of $\widehat{g}$. ■

5. CONSTRUCTIONS

For each of the examples of a reflexion-inversion space given in Section 3, one obtains corresponding constructions of hyperquasigroups.

Proposition 5.1. *Let Q be a vector space over a field F. Let G be the reflexion-inversion space of Example* 3.3. *Then a hyperquasigroup structure (Q, G) is defined by the action*

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

for x, y in Q and g in G.

Proof. The hypercommutativity and hypercancellativity may be verified directly. Certainly one has

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

the hypercommutativity. Then

$$\begin{aligned} x\,(xy\,\underline{g}\,)\,\underline{\tau g} &= x(1 - g^{-1}) + \big(x(1 - g) + yg\big)g^{-1} \\ &= x(1 - g^{-1}) + x(g^{-1} - 1) + y = y\,, \end{aligned}$$

as required for the hypercancellativity. ■

Proposition 5.2. *Let $(Q, \cdot, /, \backslash)$ be an equational quasigroup, and let G be the symmetric group S_3 on the three-element set $\{1, 2, 3\}$. Interpret G as a reflexion-inversion space according to Example* 3.4*, with reflexion $\sigma = (12)$ and inversion $\tau = (23)$. Then (Q, G) becomes a hyperquasigroup under the operations*

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

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

Proof. The hypercommutativity is immediate from the definitions, while the hypercancellativity results from the identities (XL) and (XR) for X = I, S, D. Specifically, these identities take the following form:

(IL) : $y = x\,(xy\,\underline{1})\,\underline{\tau}$

(SL) : $y = x\,(xy\,\underline{\tau})\,\underline{1}$

(IR) : $y = x\,(xy\,\underline{\sigma})\,\underline{\tau\sigma}$

(SR) : $y = x\,(xy\,\underline{\tau\sigma})\,\underline{\sigma}$

(DL) : $y = x\,(xy\,\underline{\sigma\tau})\,\underline{\tau\sigma\tau}$

(DL) : $y = x\,(xy\,\underline{\tau\sigma\tau})\,\underline{\sigma\tau}$

(recalling the equation $\sigma\tau\sigma = \tau\sigma\tau$ in S_3). Thus the hypercancellativity (4.2) is explicitly verified for each of the six elements g of G. ∎

Proposition 5.3. *Let Q be a complex vector space, and let G be the reflexion-inversion space of Example* 3.5*. Then a hyperquasigroup structure (Q, G) is defined by the action*

$$xy\,\underline{(a,b)} = xe^a + ye^b \tag{5.1}$$

for x, y in Q and (a, b) in G.

Proof. The hypercommutativity is immediate, while

$$\begin{aligned} x\left(xy\,\underline{(a,b)}\right)\underline{\tau(a,b)} &= xe^{i\pi+a-b} + (xe^a + ye^b)e^{-b} \\ &= -xe^{a-b} + xe^{a-b} + y = y \end{aligned}$$

gives the hypercancellativity. ∎

The two remaining constructions offer discrete versions of Proposition 5.3 – note the formal similarity between the corresponding hyperquasigroup actions (5.1), (5.2) and (5.3).

Proposition 5.4. *Let R be a unital ring. For an even number n, let e be a root in R of the polynomial $X^{n/2}+1$. Let Q be a unital right module over R, and let G be the reflexion-inversion space of Example* 3.6. *Then a hyperquasigroup structure (Q,G) is defined by the action*

$$xy\,\underline{(a,b)} = xe^a + ye^b \tag{5.2}$$

for x, y in Q and (a,b) in G.

Proof. Since $e^n = 1$, the action (5.2) is well-defined. The hypercommutativity is clear, while

$$\begin{aligned} x\left(xy\,\underline{(a,b)}\right)\underline{\tau(a,b)} &= xe^{a-b+n/2} + (xe^a + ye^b)e^{-b} \\ &= -xe^{a-b} + xe^{a-b} + y = y \end{aligned}$$

gives the hypercancellativity. ∎

Proposition 5.5. *Let e be an invertible element of a unital ring R of characteristic* 2. *Let Q be a unital right module over R, and let G be the reflexion-inversion space of Example* 3.7 *for the abelian group $A=\mathbb{Z}$. Then a hyperquasigroup structure (Q,G) is defined by the action*

$$xy\,\underline{(a,b)} = xe^a + ye^b \tag{5.3}$$

for x, y in Q and (a,b) in G.

Proof. Since e is invertible, the action (5.3) is well-defined. Hypercommutativity is immediate as usual, while

$$\begin{aligned} x\left(xy\,\underline{(a,b)}\right)\underline{\tau(a,b)} &= xe^{a-b} + (xe^a + ye^b)e^{-b} \\ &= xe^{a-b} + xe^{a-b} + y = y \end{aligned}$$

gives the hypercancellativity. ∎

6. From hyperquasigroups to quasigroups

According to Proposition 5.2, each quasigroup yields a hyperquasigroup. Here, it is shown that the converse is true: Hyperquasigroups yield combinatorial and equational quasigroups.

Theorem 6.1. *Let (Q, G) be a hyperquasigroup. Then for each element g of the reflexion-inversion space G, there is an equational quasigroup $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$.*

Proof. It will be shown directly that $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$ satisifies the four identities specifying equational quasigroups.

(IL): Replacing g with σg in the hypercancellativity equation (4.2) gives

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

which is exactly the identity (IL) for $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$.

(IR): The hypercancellativity equation (4.2) directly gives

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

Using hypercommutativity, this may be rewritten as

$$y = (yx\,\underline{\sigma g}\,)\,x\,\underline{\sigma\tau g}\,,$$

which is the identity (IR) for $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$.

(SL): Replacing g with $\tau\sigma g$ in the hypercancellativity equation (4.2) gives

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

which is the identity (SL) for $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$.

(SR): Replacing g with τg in the hypercancellativity equation (4.2) gives

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

Using hypercommutativity, this may be rewritten as

$$y = (yx\,\underline{\sigma\tau g}\,)\,x\,\underline{\sigma g}\,,$$

which is the identity (SR) for $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$. ∎

Corollary 6.2. *Let (Q, G) be a hyperquasigroup. Then for each element g of the reflexion-inversion space G, there is a combinatorial quasigroup $(Q, \underline{g})$.*

Proof. Replace g by σg in the statement of Theorem 6.1. ∎

Remark 6.3. In [3], James gave a characterization of combinatorial quasigroups that amounts to the invertibility of the maps $\widehat{g}$ and $\widehat{\sigma g}$ in (4.3). James' characterization could be used as an alternative direct approach to the proof of Corollary 6.2.

Example 6.4. For a finite field F of order q, consider the hyperquasigroup (Q, G) given by Proposition 5.1. Here, the combinatorial quasigroups of Corollary 6.2 constitute a set of $q - 2$ mutually orthogonal idempotent and entropic quasigroups.

Example 6.5. For a fixed (combinatorial) quasigroup $(Q, \cdot)$, consider the hyperquasigroup (Q, S_3) given by Proposition 5.2. In this case, the combinatorial quasigroups of Corollary 6.2 form the full set of conjugates of $(Q, \cdot)$.

As a consequence of the following result, it will transpire that the situation of Example 6.5 is quite typical.

Proposition 6.6. *Let (Q, G) be a hyperquasigroup. Then for all x, y in Q and g in G, one has*

$$xy\,\underline{\sigma\tau\sigma g} = xy\,\underline{\tau\sigma\tau g}\,. \tag{6.1}$$

Proof. Consider the equational quasigroup $(Q, \underline{\sigma g}, \underline{\sigma\tau g}, \underline{\tau\sigma g})$ given by Theorem 6.1. The identity (DL) in this equational quasigroup takes the form

$$y = x\,(yx\,\underline{\tau\sigma g}\,)\,\underline{\sigma\tau g}\,,$$

which may be rewritten as

$$y = x\,(xy\,\underline{\sigma\tau\sigma g}\,)\,\underline{\sigma\tau g} \tag{6.2}$$

using hypercommutativity. On the other hand, the hypercancellation equation (4.2) with g replaced by $\tau\sigma\tau g$ yields

$$y = x\,(xy\,\underline{\tau\sigma\tau g}\,)\,\underline{\sigma\tau g}\,. \tag{6.3}$$

Since $(Q, \underline{\sigma\tau g})$ is a combinatorial quasigroup (in which the equation $y = xz\,\underline{\sigma\tau g}$ has a unique solution z for given x and y), (6.2) and (6.3) together yield the desired result (6.1). ∎

For a hyperquasigroup (Q, G), consider the algebra $(Q, \underline{G})$, the underlying set Q endowed with the set $\underline{G} = \{\underline{g} \mid g \in G\}$ of binary operations. The action of the involutions σ and τ on the reflexion-inversion space G yields an action on the binary operation set $\underline{G}$. Proposition 6.6 shows that the action of σ and τ on $\underline{G}$ is an S_3-action. For each element g of G, the elements $\underline{g'}$ of the orbit $\underline{S_3 g}$ of $\underline{g}$ under this S_3-action form the full set of quasigroup operations conjugate to the combinatorial quasigroup operation $\underline{g}$ on Q. One may summarize as follows.

Theorem 6.7. *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.

Between them, Proposition 5.2 and Theorem 6.7 give a complete description of the relationship between quasigroups and hyperquasigroups.

Acknowledgement

The author gratefully acknowledges the hospitality of the Faculty of Mathematics and Information Sciences of Warsaw University of Technology during the preparation of this paper while he was on a Faculty Professional Development Assignment from Iowa State University.

REFERENCES

[1] L. Euler, *Recherches sur une nouvelle espèce de carrés magiques*, Mém. de la Societé de Vlissingue **9** (1779), pp. 85 ff.

[2] T. Evans, *Homomorphisms of non-associative systems*, J. London Math. Soc. **24** (1949), 254–260.

[3] I.M. James, *Quasigroups and topology*, Math. Zeitschr. **84** (1964), 329–342.

[4] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[5] A. Sade, *Quasigroupes obéissant à certaines lois*, Rev. Fac. Sci. Univ. Istanbul, Ser. A **22** (1957), 151–184.

[6] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[7] W. Taylor, *Hyperidentities and hypervarieties*, Aequationes Math. **23** (1981), 30–49.

Received 27 February 2006
Revised 31 March 2006