

Ternary quasigroups and the modular group

JONATHAN D.H. SMITH

Abstract. For a positive integer n , the usual definitions of n -quasigroups are rather complicated: either by combinatorial conditions that effectively amount to Latin n -cubes, or by $2n$ identities on $n + 1$ different n -ary operations. In this paper, a more symmetrical approach to the specification of n -quasigroups is considered. In particular, ternary quasigroups arise from actions of the modular group.

Keywords: quasigroup, ternary quasigroup, n -quasigroup, heterogeneous algebra, hyperidentity, modular group, conjugate, parastrophe, time reversal

Classification: Primary 20N05; Secondary 08A68

1. Quasigroups

For a positive integer n , a (*combinatorial*) n -*quasigroup* is a set Q equipped with an n -ary *multiplication* operation

$$\mu : Q^n \rightarrow Q; (x_n, \dots, x_1) \mapsto x_n \dots x_1 \mu$$

such that, for an $(n + 1)$ -tuple

$$(1.1) \quad (x_n, \dots, x_1, x_0)$$

of elements of Q required to satisfy the condition

$$(1.2) \quad x_n \dots x_1 \mu = x_0,$$

specification of any n coordinates of (1.1) determines the remaining one uniquely. Note that a combinatorial 1-quasigroup is just a set Q with a permutation (self-bijection) $\mu : Q \rightarrow Q$, or in other words a dynamical system with state space Q and invertible transition operator μ .

For each index $1 \leq i \leq n$, and for each choice $x_n, \dots, x_{i+1}, x_{i-1}, \dots, x_1$ of fixed elements of an n -quasigroup Q , a *translation*

$$(1.3) \quad T_i(x_n, \dots, x_{i+1}, x_{i-1}, \dots, x_1) : Q \rightarrow Q; x_i \mapsto x_n \dots x_1 \mu$$

is defined. The combinatorial definition of an n -quasigroup means precisely that each translation is a permutation of the underlying set Q .

The combinatorial definition of n -quasigroups may be reformulated in algebraic terms of operations and identities. An (equational) n -quasigroup $(Q, \mu, \mu^1, \dots, \mu^n)$ is a set Q equipped with n -ary operations μ, μ^1, \dots, μ^n satisfying the identities

$$(1.4) \quad x_n \dots x_{i+1} (x_n \dots x_1 \mu) x_{i-1} \dots x_1 \mu^i = x_i$$

and

$$(1.5) \quad x_n \dots x_{i+1} (x_n \dots x_1 \mu^i) x_{i-1} \dots x_1 \mu = x_i$$

for each $1 \leq i \leq n$. The operations μ^1, \dots, μ^n are described as *divisions*. Note that the identity (1.4) gives the injectivity of the translation (1.3), while (1.5) gives its surjectivity. Thus each equational n -quasigroup $(Q, \mu, \mu^1, \dots, \mu^n)$ yields a combinatorial n -quasigroup (Q, μ) . Conversely, a combinatorial n -quasigroup (Q, μ) yields an equational n -quasigroup $(Q, \mu, \mu^1, \dots, \mu^n)$, defining

$$x_n \dots x_{i+1} x_0 x_{i-1} \dots x_1 \mu^i = x_i$$

if and only if (1.2) holds.

2. Groups

For a positive integer n , consider the group M_n presented as

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

In other words, M_n is the free product of two cyclic groups, one $\langle \sigma \rangle$ of order n , and one $\langle \tau \rangle$ of order 2.

Example 2.1. For $n = 1$, M_1 is just the cyclic group $\langle \tau \rangle$ of order 2.

Example 2.2. For $n = 2$, M_2 is the *infinite dihedral group* ([2, p. 133]). Recall that the *dihedral group* D_d of degree d and order $2d$ (the group of symmetries of the regular d -gon) may be presented as

$$(2.1) \quad \langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^d = 1 \rangle$$

([2, (1.53)]).

Example 2.3. For $n = 3$, M_3 is the *modular group* $\mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$ ([8, p. 128]). For each element

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

of $\mathrm{SL}_2(\mathbb{Z})$, a matrix of determinant 1 with integral entries, write the corresponding coset $\{\pm A\}$ in M_3 as

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right\}.$$

Setting

$$\sigma = \begin{Bmatrix} 0 & -1 \\ 1 & 1 \end{Bmatrix} \quad \text{and} \quad \tau = \begin{Bmatrix} 0 & -1 \\ 1 & 0 \end{Bmatrix},$$

one has $\sigma^3 = \tau^2 = 1$, and $\text{SL}_2(\mathbb{Z})/\{\pm I_2\}$ is generated freely by σ and τ , subject to these order relations ([2, (7.25)], [8, p. 131]).

Lemma 2.4. *Consider the symmetric group $S_{n+1} = \{0, 1, \dots, n\}!$.*

- (a) *For $n \geq 1$, the group S_{n+1} is a quotient of M_n .*
- (b) $S_3 = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^3 = 1 \rangle$.
- (c) $S_4 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = (\sigma\tau)^4 = 1 \rangle$.

PROOF: (a): Apply the First Isomorphism Theorem to the surjective homomorphism

$$(2.2) \quad r : M_n \rightarrow S_{n+1}; \quad \sigma \mapsto (1 \ 2 \ \dots \ n), \quad \tau \mapsto (0 \ 1).$$

(b): This is the case $d = 3$ of (2.1).

(c): See [2, (1.59)]. □

3. Spaces

For a positive integer n , an n -ary space (G, σ, τ) is a set G equipped with maps

$$(3.1) \quad \sigma : G \rightarrow G; \quad g \mapsto \sigma g$$

and

$$(3.2) \quad \tau : G \rightarrow G; \quad g \mapsto \tau g$$

satisfying $\sigma^n = \tau^2 = 1$. The map σ is known as the *shift*, while the map τ is known as the *inversion*. Note that n -ary spaces are left M_n -sets.

Example 3.1. For each positive integer n , each set G furnishes a trivial n -ary space, on which both σ and τ are the identity map id_G .

Example 3.2. For $n=1$, each group G provides a unary space, with $\tau g = g^{-1}$ for g in G .

Example 3.3. For $n=2$, the binary spaces are the *reflexion-inversion spaces* of [9], the shift being described as *reflexion* in this case.

- (a) For a field F , take $G = F \setminus \{0, 1\}$. Then G is a binary space, with $\sigma g = 1 - g$ and $\tau g = g^{-1}$ for points g of G ([9, Example 3.3]).
- (b) The symmetric group S_3 is a binary space. Taking $\sigma = (1 \ 2)$ and $\tau = (0 \ 1)$, the maps (3.1) and (3.2) are interpreted as left multiplications within S_3 — compare Lemma 2.4(b).

Example 3.4. The symmetric group S_4 is a ternary space. Taking $\sigma = (1\ 2\ 3)$ and $\tau = (0\ 1)$, the maps (3.1) and (3.2) are interpreted as left multiplications within S_4 — compare Lemma 2.4(c).

Example 3.5. Let R be a unital ring, and let U be a group of units in R . For a positive integer n , consider $G = U^n$. Define

$$\sigma(u_n, \dots, u_2, u_1) = (u_{n-1}, \dots, u_1, u_n)$$

and

$$\tau(u_n, \dots, u_2, u_1) = (-u_n u_1^{-1}, \dots, -u_2 u_1^{-1}, u_1^{-1})$$

for a point (u_n, \dots, u_1) of G . Then G becomes an n -ary space.

4. Hyperquasigroups

For a positive integer n , an n -hyperquasigroup (or n -ary hyperquasigroup) is a pair (Q, G) consisting of a set Q and an n -ary space G , with an n -ary action

$$(4.1) \quad Q^n \times G \rightarrow Q; (x_n, \dots, x_1, g) \mapsto x_n \dots x_1 \underline{g}$$

of G on Q , such that the (n) -hypercommutative law

$$(4.2) \quad x_n \dots x_2 x_1 \underline{g} = x_{n-1} \dots x_1 x_n \underline{\sigma g}$$

and the (n) -hypercancellation law

$$(4.3) \quad x_n \dots x_2 (x_n \dots x_1 \underline{g}) \underline{\tau g} = x_1$$

are satisfied for all x_1, \dots, x_n in Q and g in G .

Remark 4.1. A hyperquasigroup (Q, G) may be construed as a two-sorted or heterogeneous algebra ([4], [6]), with the n -ary space operations σ and τ on the sort G , and (4.1) as a third operation.

Example 4.2. For each positive integer n , and for each n -ary space G , the empty set forms an n -hyperquasigroup (\emptyset, G) . The actions (4.1) reduce to id_\emptyset .

Example 4.3. For each positive integer n , consider the trivial n -ary space \emptyset as in Example 3.1. Let Q be a set. Then (Q, \emptyset) forms an n -hyperquasigroup, with (4.1) as the insertion $\emptyset \hookrightarrow Q$. The hypercommutativity (4.2) and hypercancellation (4.3) are vacuously satisfied.

Example 4.4. For $n = 1$, let G be a group, construed as a unary space according to Example 3.2. Consider a right G -set Q . For g in G and x in Q , define the unary action $x \underline{g} = xg$. The hypercommutativity is trivial, while the hypercancellation is just $(xg)g^{-1} = x$. Thus (Q, G) is a unary hyperquasigroup.

Example 4.5. For each positive integer n , consider the trivial n -ary space $\{1\}$.

- (a) For $n = 1$, each set Q forms a unary hyperquasigroup $(Q, \{1\})$ as a $\{1\}$ -set for the trivial group $\{1\}$, according to Example 4.4.
- (b) For $n = 2$, a binary hyperquasigroup $(Q, \{1\})$ is just a totally symmetric quasigroup, with multiplication $x_1x_2\underline{1}$.
- (c) For any positive n , let Q be an abelian group of exponent 2. Then $(Q, \{1\})$ forms an n -hyperquasigroup with

$$x_1x_2 \dots x_n\underline{1} = x_1x_2 \dots x_n$$

for x_1, \dots, x_n in Q .

Example 4.6. For $n = 2$, binary hyperquasigroups reduce to hyperquasigroups in the sense of [9].

- (a) For a field F , consider the binary space $G = F \setminus \{0, 1\}$ of Example 3.3(a). For a vector space Q over F , define the binary action

$$Q^2 \times G \rightarrow Q; (x_2, x_1, g) \mapsto x_2(1 - g) + x_1g.$$

Then (Q, G) forms a binary hyperquasigroup ([9, Proposition 5.1]).

- (b) Let $(Q, \cdot, /, \backslash)$ be a (binary) quasigroup, and let $G = S_3$, construed as a binary space according to Example 3.3(b). Then (Q, G) is a binary hyperquasigroup under the operations

$$\begin{aligned} xy\underline{1} &= x \cdot y, & xy\underline{\sigma\tau\sigma} &= x/y, & xy\underline{\tau} &= x \backslash y, \\ xy\underline{\sigma} &= y \cdot x, & xy\underline{\tau\sigma} &= y/x, & xy\underline{\sigma\tau} &= y \backslash x \end{aligned}$$

([9, Proposition 5.2]).

Example 4.7. For a positive integer n and a unital ring R , consider the n -ary space G of Example 3.5. Let Q be a unital right R -module. Define the n -ary action

$$x_n \dots x_1 \underline{(u_n, \dots, u_1)} = x_nu_n + \dots + x_1u_1$$

for x_i in Q and (u_n, \dots, u_1) in G . Then (Q, G) is an n -ary hyperquasigroup.

The meaning of hypercommutativity in an n -hyperquasigroup is immediate. The significance of hypercancellation is interpreted as follows (compare [5], [9] for the binary case).

Proposition 4.8. *Let (Q, G) be an n -hyperquasigroup. For each point g in G , define*

$$\widehat{g}: Q^n \rightarrow Q^n; (x_n, \dots, x_2, x_1) \mapsto (x_n, \dots, x_2, x_n \dots x_1\underline{g}).$$

Then $\widehat{\tau\widehat{g}}$ is the two-sided inverse of \widehat{g} in the semigroup of selfmaps on the set Q^n .

PROOF: The equation $\widehat{g}\widehat{\tau\widehat{g}} = \text{id}_{Q^n}$ is immediate from (4.3), while $\widehat{\tau\widehat{g}}\widehat{g} = \text{id}_{Q^n}$ follows from (4.3) with g replaced by τg , recalling $\tau\tau g = g$. □

Remark 4.9. For an n -ary operation

$$Q^n \rightarrow Q; (x_n, \dots, x_1) \mapsto x_n \dots x_1 \omega$$

on a set Q , the invertibility of the map

$$\widehat{\omega} : Q^n \rightarrow Q^n; (x_n, \dots, x_2, x_1) \mapsto (x_n, \dots, x_2, x_n \dots x_1 \omega)$$

does not mean that (Q, ω) is a (combinatorial) n -quasigroup. For example, the binary projection

$$\pi_1 : Q^2 \rightarrow Q; (x_0, x_1) \mapsto x_1$$

has $\widehat{\pi_1} = \text{id}_{Q^2}$.

5. From hyperquasigroups to quasigroups

By Proposition 4.5 and Remark 4.9, hypercancellativity alone is insufficient for a quasigroup. The following theorem shows that quasigroups are obtained from the combination of hypercommutativity and hypercancellativity. The binary case appeared as [9, Theorem 6.1]. The proof of the general case given here is conceptually simpler, although the details are more complex.

Theorem 5.1. *For a positive integer n , let (Q, G) be an n -hyperquasigroup. Then for each element g of the n -ary space G , there is an equational n -quasigroup*

$$\left(Q, \underline{g}, \underline{\tau g}, \dots, \underline{\sigma^{i-1} \tau \sigma^{1-i} g}, \dots, \underline{\sigma^{n-1} \tau \sigma^{1-n} g} \right)$$

with multiplication \underline{g} and divisions $\underline{\sigma^{i-1} \tau \sigma^{1-i} g}$ for $1 \leq i \leq n$.

PROOF: The identities (1.4) and (1.5) must be established for $1 \leq i \leq n$, with $\mu = \underline{g}$ and $\mu^i = \underline{\sigma^{i-1} \tau \sigma^{1-i} g}$. Consider the hypercancellativity

$$(5.1) \quad x_n \dots x_2 (x_n \dots x_1 \underline{g}) \underline{\tau g} = x_1$$

as in (4.3). Applying hypercommutativity $i - 1$ times to the inner operation of (5.1) yields

$$x_n \dots x_2 \left(x_{n-(i-1)} \dots x_2 x_1 x_n \dots x_{n-(i-2)} \underline{\sigma^{i-1} g} \right) \underline{\tau g} = x_1.$$

Applying hypercommutativity $i - 1$ times to the outer operation then gives

$$\begin{aligned} x_{n-(i-1)} \dots x_2 \left(x_{n-(i-1)} \dots x_2 x_1 x_n \dots x_{n-(i-2)} \underline{\sigma^{i-1} g} \right) x_n \dots \\ \dots x_{n-(i-2)} \underline{\sigma^{i-1} \tau g} = x_1. \end{aligned}$$

Replacing x_k by

$$\begin{cases} x_{k+(i-1)} & \text{for } 1 \leq k \leq n - (i - 1), \\ x_{k+(i-1)-n} & \text{for } n - (i - 2) \leq k \leq n \end{cases}$$

yields

$$(5.2) \quad x_n \dots x_{i+1} \left(x_n \dots x_1 \underline{\sigma^{i-1}g} \right) x_{i-1} \dots x_1 \underline{\sigma^{i-1}\tau g} = x_i.$$

Replace g in (5.2) by $\sigma^{1-i}g$ to obtain

$$x_n \dots x_{i+1} \left(x_n \dots x_1 \underline{g} \right) x_{i-1} \dots x_1 \underline{\sigma^{i-1}\tau\sigma^{1-i}g} = x_i,$$

which is (1.4). Finally, replace g in (5.2) by $\tau\sigma^{1-i}g$ to obtain

$$x_n \dots x_{i+1} \left(x_n \dots x_1 \underline{\sigma^{i-1}\tau\sigma^{1-i}g} \right) x_{i-1} \dots x_1 \underline{g} = x_i,$$

which is (1.5). □

Corollary 5.2. *For a positive integer n , let (Q, G) be an n -hyperquasigroup. Then each point g of the n -ary space G yields a combinatorial n -quasigroup (Q, \underline{g}) .*

6. The structure theorem

Let n be a positive integer. In the symmetric group $S_{n+1} = \{0, 1, \dots, n\}!$, consider the involution

$$\alpha = (2 \ n)(3 \ n-1) \dots \begin{cases} \dots \left(\frac{n}{2} \ \frac{n+4}{2} \right), & n \text{ even;} \\ \dots \left(\frac{n+1}{2} \ \frac{n+3}{2} \right), & n \text{ odd.} \end{cases}$$

Define a surjective homomorphism

$$(6.1) \quad M_n \rightarrow S_{n+1}; \quad \pi \mapsto \bar{\pi}$$

by concatenating the surjective homomorphism r of (2.2) with conjugation by the permutation α in S_{n+1} . In particular,

$$(6.2) \quad \bar{\sigma} = (1 \ 2 \ \dots \ n)^\alpha = (1 \ n \ \dots \ 2)$$

and

$$(6.3) \quad \bar{\tau} = (0 \ 1)^\alpha = (0 \ 1).$$

Lemma 6.1. *Let (Q, G) be an n -hyperquasigroup. Then*

$$(6.4) \quad x_n \dots x_2 x_1 \underline{g} = x_0 \quad \Leftrightarrow \quad x_{n\bar{\pi}} \dots x_{2\bar{\pi}} x_{1\bar{\pi}} \underline{\pi g} = x_{0\bar{\pi}}$$

for each element π of M_n , point g in G , and elements x_0, \dots, x_n of Q .

PROOF: The equivalence (6.4) holds trivially for $\pi = 1$. Suppose that it holds for a certain element π of M_n . Then

$$\begin{aligned} & x_{n\bar{\pi}} \dots x_{2\bar{\pi}} x_{1\bar{\pi}} \underline{\pi g} = x_{0\bar{\pi}} \\ \Leftrightarrow & x_{(n-1)\bar{\pi}} \dots x_{1\bar{\pi}} x_{n\bar{\pi}} \underline{\sigma \pi g} = x_{0\bar{\pi}} \\ \Leftrightarrow & x_{n\bar{\sigma\pi}} \dots x_{2\bar{\sigma\pi}} x_{1\bar{\sigma\pi}} \underline{\sigma \pi g} = x_{0\bar{\sigma\pi}} \end{aligned}$$

by the hypercommutativity (4.2) and (6.2). Thus the equivalence (6.4) holds for $\sigma\pi$ in M_n . Again,

$$\begin{aligned} & x_{n\bar{\pi}} \dots x_{2\bar{\pi}} x_{1\bar{\pi}} \underline{\pi g} = x_{0\bar{\pi}} \\ \Leftrightarrow & x_{n\bar{\pi}} \dots x_{2\bar{\pi}} x_{0\bar{\pi}} \underline{\tau \pi g} = x_{1\bar{\pi}} \\ \Leftrightarrow & x_{n\bar{\tau\pi}} \dots x_{2\bar{\tau\pi}} x_{1\bar{\tau\pi}} \underline{\pi g} = x_{0\bar{\tau\pi}} \end{aligned}$$

by the hypercancellativity (4.3) and (6.3) Thus the equivalence (6.4) holds for $\tau\pi$ in M_n . By induction, it follows that the equivalence (6.4) holds for each element of M_n . □

Let (Q, G) be an n -hyperquasigroup. Set

$$\underline{G} = \{ \underline{g} : Q^n \rightarrow Q \mid g \in G \}.$$

By Lemma 6.1, the action

$$M_n \rightarrow \underline{G}!; \pi \mapsto (\underline{g} \mapsto \underline{\pi g})$$

factorizes through the homomorphism (6.1) to S_{n+1} . Thus the set \underline{G} of n -ary operations on Q is an S_{n+1} -set. For a point g in the space G , Corollary 5.2 yields n -quasigroups $(Q, \underline{\pi g})$ given by the S_{n+1} -orbit of \underline{g} . The various n -quasigroups in a given orbit are described as mutual *conjugates* or *parastrophes*. For binary quasigroups, these concepts are well known ([1, Example II.6.1], [7]). For unary quasigroups, as invertible dynamical systems, conjugation corresponds to time reversal.

The structure of (Q, \underline{G}) may now be summarized as follows (compare [9, Theorem 6.7] for the binary case).

Theorem 6.2. *Let n be a positive integer. Then each n -hyperquasigroup (Q, G) yields an algebra structure (Q, \underline{G}) consisting of the union of mutually disjoint sets of conjugate n -quasigroup operations.*

Remark 6.3. Let $(Q, \varphi, \varphi^1, \dots, \varphi^n)$ be an n -quasigroup. Consider M_n as an n -ary space (M_n, σ, τ) given by the free left M_n -set, so that the actions (3.1) and (3.2) are the left multiplications by σ and τ in the group M_n . Use the specification

$$x_n \dots x_2 x_1 \underline{1} = x_n \dots x_2 x_1 \varphi$$

together with (6.4) to define an n -ary action of M_n on Q . A comparison with Theorem 5.1 and its proof shows that

$$\varphi^i = \underline{\sigma^{i-1} \tau \sigma^{1-i}}$$

for $1 \leq i \leq n$. One then obtains (Q, M_n) as a hyperquasigroup. Within this hyperquasigroup, the n -quasigroup $(Q, \underline{1})$ yielded by Theorem 5.1 realizes the given n -quasigroup (Q, φ) . By Theorem 6.2, the n -quasigroups (Q, \underline{g}) for g in M_n are the conjugates of (Q, φ) .

Acknowledgment. Thanks are due to an anonymous referee for valuable comments on an earlier version of this paper.

REFERENCES

- [1] Chein O. et al., *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.
- [2] Coxeter H.S.M., Moser W.O.J., *Generators and Relations for Discrete Groups*, Springer, Berlin, 1957.
- [3] Evans T., *Homomorphisms of non-associative systems*, J. London Math. Soc. **24** (1949), 254–260.
- [4] Higgins P.J., *Algebras with a scheme of operators*, Math. Nachr. **27** (1963), 115–132.
- [5] James I.M., *Quasigroups and topology*, Math. Z. **84** (1964), 329–342.
- [6] Lügowski H., *Grundzüge der Universellen Algebra*, Teubner, Leipzig, 1976.
- [7] Sade A., *Quasigroupes obéissant à certaines lois*, Rev. Fac. Sci. Univ. Istanbul, Ser. A **22** (1957), 151–184.
- [8] Serre, J.-P., *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970.
- [9] Smith J.D.H., *Axiomatization of quasigroups*, Discuss. Math. Gen. Algebra Appl. **27** (2007), 21–33.

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IOWA 50011-2064, U.S.A.

E-mail: jdsmith@math.iastate.edu

URL: <http://orion.math.iastate.edu/jdsmith/>

(Received September 14, 2007, revised November 4, 2007)