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

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

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

$$
(x_n, \ldots, x_1, x_0)
$$

of elements of $Q$ required to satisfy the condition

$$
x_n \ldots x_1 \mu = x_0,
$$

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 $\mu$.

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

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

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 \( ( \text{equational} ) \) \( n \)-quasigroup \( (Q, \mu, \mu^1, \ldots, \mu^n) \) is a set \( Q \) equipped with \( n \)-ary operations \( \mu, \mu^1, \ldots, \mu^n \) satisfying the identities

\[
x_n \ldots x_{i+1} (x_n \ldots x_1 \mu) x_{i-1} \ldots x_1 \mu^i = x_i
\]

for each \( 1 \leq i \leq n \). The operations \( \mu^1, \ldots, \mu^n \) are described as \( \text{divisions} \). 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 \( (Q, \mu, \mu^1, \ldots, \mu^n) \) yields a combinatorial \( n \)-quasigroup \( (Q, \mu) \). Conversely, a combinatorial \( n \)-quasigroup \( (Q, \mu) \) yields an equational \( n \)-quasigroup \( (Q, \mu, \mu^1, \ldots, \mu^n) \), defining

\[
x_n \ldots x_{i+1} x_0 x_{i-1} \ldots x_1 \mu^i = x_i
\]

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 \textit{infinite dihedral group} ([2, p.133]). Recall that the \textit{dihedral group} \( D_d \) of degree \( d \) and order \( 2d \) (the group of symmetries of the regular \( d \)-gon) may be presented as

\[
\langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma \tau)^d = 1 \rangle
\]

([2, (1.53)]).

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

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

of \( \text{SL}_2(\mathbb{Z}) \), 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

\[ \sigma = \begin{cases} 0 & -1 \\ 1 & 1 \end{cases} \quad \text{and} \quad \tau = \begin{cases} 0 & -1 \\ 1 & 0 \end{cases}, \]

one has \( \sigma^3 = \tau^2 = 1 \), and \( SL_2(\mathbb{Z})/\{ \pm I_2 \} \) is generated freely by \( \sigma \) and \( \tau \), subject to these order relations ([2, (7.25)], [8, p.131]).

**Lemma 2.4.** Consider the symmetric group \( S_{n+1} = \{0, 1, \ldots, n\}! \).

(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

\[ r : M_n \rightarrow S_{n+1}; \; \sigma \mapsto (1 \ 2 \ \ldots \ n), \; \tau \mapsto (0 \ 1). \]

(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 \( (G, \sigma, \tau) \) is a set \( G \) equipped with maps

\[ \sigma : G \to G; \; g \mapsto \sigma g \]

and

\[ \tau : G \to G; \; g \mapsto \tau g \]

satisfying \( \sigma^n = \tau^2 = 1 \). The map \( \sigma \) is known as the *shift*, while the map \( \tau \) 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 \( \sigma \) and \( \tau \) are the identity map \( \text{id}_G \).

**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 *reflection-inversion spaces* of [9], the shift being described as *reflection* 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

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

and

$$\tau(u_n, \ldots, u_2, u_1) = (-u_nu_1^{-1}, \ldots, -u_2u_1^{-1}, u_1^{-1})$$

for a point $(u_n, \ldots, u_1)$ 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

$$Q^n \times G \rightarrow Q; \ (x_n, \ldots, x_1, g) \mapsto x_n \ldots x_1g$$

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

$$x_n \ldots x_2 x_1 g = x_{n-1} \ldots x_1 x_n \sigma g$$

and the (n-)hypercancellation law

$$x_n \ldots x_2(x_n \ldots x_1 g) \tau g = x_1$$

are satisfied for all $x_1, \ldots, x_n$ 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 $\sigma$ and $\tau$ 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 $\text{id}_\emptyset$.

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 $\emptyset \mapsto Q$. 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 $xg = xg$. 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

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

for $x_1, \ldots, x_n$ 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

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

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

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

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

([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

$$x_n \ldots x_1(u_n, \ldots, u_1) = x_nu_n + \ldots + x_1u_1$$

for $x_i$ in $Q$ and $(u_n, \ldots, u_1)$ 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

$$\hat{g} : Q^n \to Q^n; \ (x_n, \ldots, x_2, x_1) \mapsto (x_n, \ldots, x_2, x_n \ldots x_1g).$$

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

**Proof:** The equation $\hat{g} \hat{\tau g} = \text{id}_{Q^n}$ is immediate from (4.3), while $\hat{\tau g} \hat{g} = \text{id}_{Q^n}$ follows from (4.3) with $g$ replaced by $\tau g$, recalling $\tau \tau g = g$. \qed
Remark 4.9. For an \( n \)-ary operation

\[
Q^n \to Q; \ (x_n, \ldots, x_1) \mapsto x_n \ldots x_1 \omega
\]
on a set \( Q \), the invertibility of the map

\[
\widehat{\omega}: Q^n \to Q^n; \ (x_n, \ldots, x_2, x_1) \mapsto (x_n, \ldots, x_2, x_n \ldots x_1 \omega)
\]
does not mean that \((Q, \omega)\) is a (combinatorial) \( n \)-quasigroup. For example, the binary projection

\[
\pi_1: Q^2 \to Q; \ (x_0, x_1) \mapsto x_1
\]
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

\[
(Q, g, \tau g, \ldots, \sigma^{i-1}\tau \sigma^{1-i}g, \ldots, \sigma^{n-1}\tau \sigma^{1-n}g)
\]
with multiplication \( g \) and divisions \( \sigma^{i-1}\tau \sigma^{1-i}g \) for \( 1 \leq i \leq n \).

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

\[
x_n \ldots x_2 \left(x_n \ldots x_1 g \right) \tau g = x_1
\]
as in (4.3). Applying hypercommutativity \( i - 1 \) times to the inner operation of (5.1) yields

\[
x_n \ldots x_2 \left(x_n-(i-1) \ldots x_2 x_1 x_n \ldots x_n-(i-2) \sigma^{i-1}g \right) \tau g = x_1.
\]

Applying hypercommutativity \( i - 1 \) times to the outer operation then gives

\[
x_n-(i-1) \ldots x_2 \left(x_n-(i-1) \ldots x_2 x_1 x_n \ldots x_n-(i-2) \sigma^{i-1}g \right) x_n \ldots
\]

\[\ldots x_n-(i-2) \sigma^{i-1} \tau g = x_1.\]
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

\[x_n \ldots x_{i+1} \left( x_n \ldots x_1 \sigma_{i-1}^{-1} g \right) x_{i-1} \ldots x_1 \sigma_{i-1}^{-1} \tau g = x_i.\] (5.2)

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

\[x_n \ldots x_{i+1} \left( x_n \ldots x_1 g \right) x_{i-1} \ldots x_1 \sigma_{i-1}^1 \tau \sigma_{1-i}^1 g = x_i,
\]
which is (1.4). Finally, replace $g$ in (5.2) by $\tau \sigma_{1-i}^1 g$ to obtain

\[x_n \ldots x_{i+1} \left( x_n \ldots x_1 \sigma_{1-i}^1 \tau \sigma_{1-i}^1 g \right) x_{i-1} \ldots x_1 g = x_i,
\]
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 $(Q, g)$.

6. The structure theorem

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

\[
\alpha = (2 n)(3 n-1) \ldots \begin{cases}
\ldots (n \frac{n+4}{2}), & n \text{ even}; \\
\ldots (n+1 \frac{n+3}{2}), & n \text{ odd}.
\end{cases}
\]

Define a surjective homomorphism

\[M_n \rightarrow S_{n+1}; \pi \mapsto \overline{\pi}\]

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

\[\overline{\sigma} = (1 2 \ldots n)^{\alpha} = (1 n \ldots 2)\] (6.2)
and

\[\overline{\tau} = (0 1)^{\alpha} = (0 1).\] (6.3)
Lemma 6.1. Let \((Q, G)\) be an \(n\)-hyperquasigroup. Then

\[ x_n \ldots x_2 x_1 g = x_0 \iff x_{n\pi} \ldots x_{2\pi} x_{1\pi} \pi g = x_{0\pi} \]

for each element \(\pi\) of \(M_n\), point \(g\) in \(G\), and elements \(x_0, \ldots, x_n\) of \(Q\).

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

\[ x_{n\pi} \ldots x_{2\pi} x_{1\pi} \pi g = x_{0\pi} \iff x_{(n-1)\pi} \ldots x_{1\pi} x_{n\pi} \sigma \pi g = x_{0\pi} \]
\[ \iff x_{n\sigma \pi} \ldots x_{2\sigma \pi} x_{1\sigma \pi} \sigma \pi g = x_{0\sigma \pi} \]

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

\[ x_{n\pi} \ldots x_{2\pi} x_{1\pi} \pi g = x_{0\pi} \iff x_{n\pi} \ldots x_{2\pi} x_{0\pi} \tau \pi g = x_{1\pi} \]
\[ \iff x_{n\tau \pi} \ldots x_{2\tau \pi} x_{1\tau \pi} \tau \pi g = x_{0\tau \pi} \]

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 \(M_n\). \(\square\)

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

\[ G = \{g : Q^n \to Q \mid g \in G\} \]

By Lemma 6.1, the action

\[ M_n \to G!; \quad \pi \mapsto (g \mapsto \pi g) \]

factorizes through the homomorphism (6.1) to \(S_{n+1}\). Thus the set \(G\) 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 \((Q, \pi g)\) given by the \(S_{n+1}\)-orbit of \(g\). 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 \((Q, G)\) 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 \((Q, \bar{G})\) consisting of the union of mutually disjoint sets of conjugate \(n\)-quasigroup operations.
Remark 6.3. Let \((Q, \varphi, \varphi^1, \ldots, \varphi^n)\) be an \(n\)-quasigroup. Consider \(M_n\) as an \(n\)-ary space \((M_n, \sigma, \tau)\) given by the free left \(M_n\)-set, so that the actions (3.1) and (3.2) are the left multiplications by \(\sigma\) and \(\tau\) in the group \(M_n\). Use the specification
\[
x_n \ldots x_2 x_1 \varphi = x_n \ldots x_2 x_1 \varphi
\]
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
\[
\varphi^i = \sigma^{i-1} \tau \sigma^{1-i}
\]
for \(1 \leq i \leq n\). One then obtains \((Q, M_n)\) as a hyperquasigroup. Within this hyperquasigroup, the \(n\)-quasigroup \((Q, 1)\) yielded by Theorem 5.1 realizes the given \(n\)-quasigroup \((Q, \varphi)\). By Theorem 6.2, the \(n\)-quasigroups \((Q, g)\) for \(g\) in \(M_n\) are the conjugates of \((Q, \varphi)\).

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

References


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

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

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