Quasigroups and Related Systems **16** (2008), 103 – 118

Greedy quasigroups

Theodore A. Rice

Abstract

The paper investigates the quasigroup Q_s constructed on the well-ordered set of natural numbers by placing a number s known as the *seed* in the top left-hand corner of the body of the multiplication table, and then completing the Latin square using the greedy algorithm that chooses the least possible entry at each stage. The initial motivation comes from the theory of combinatorial games, where Q_0 gives the usual nim sum, while Q_1 gives the corresponding sums for positions in misère nim. The multiplication groups of these quasigroups are analyzed. The alternating group of the natural numbers is a subgroup of the multiplication groups. It is shown that these so-called *greedy quasigroups* Q_s are mutually non-isomorphic. The quasigroup Q_1 is subdirectly irreducible. For $s > 1$, the greedy quasigroups Q_s are simple, and for $s > 2$ they are rigid, possessing no non-trivial automorphisms. Indeed in this case the endomorphism monoid contains just the identity and a single constant. The subquasigroup structures of the Q_s are also determined. While Q_0, Q_1 have uncountably many subquasigroups, and Q_2 has just one proper, non-trivial subquasigroup, Q_s has none for $s > 2$.

1. Introduction

In this paper, quasigroups motivated by combinatorial games, nim in particular, are examined. They form a countably infinite family of infinite quasigroups with some curious properties. The underlying set Q of the quasigroups is taken to be the well-ordered set of natural numbers including 0. A quasigroup is constructed by filling in the multiplication table in a greedy fashion with the rows and columns labelled by the elements of Q in their natural order. For each proper subset S, of Q, define the *minimal*

2000 Mathematics Subject Classification: 20N05, 91A46
Keywords: quasigroup, combinatorial game

excluded number $\operatorname{mex} S$ of S to be the least element of the (non-empty) complement of S in Q. (This element is uniquely defined by the well-ordering principle.) Fix a natural number s, known as the *seed*. Define

$$0 \cdot 0 := s. \tag{1}$$

One may then use the following greedy algorithm to define the remaining products of natural numbers l and m inductively:

$$l \cdot m := \operatorname{mex}(\{i \cdot m \mid i < l\} \cup \{l \cdot j \mid j < m\}). \tag{2}$$

The algorithm guarantees that the body of the multiplication table will be a (infinite) Latin square, and therefore that $(Q, \cdot)$ becomes a quasigroup Q_s, known as the *greedy quasigroup* seeded by s. As an illustration, the following table

	0	1	2	3	4	5	6	7	8	9	10
0	5	0	1	2	3	4	6	7	8	9	10
1	0	1	2	3	4	5	7	6	9	8	11
2	1	2	0	4	5	3	8	9	6	7	12
3	2	3	4	0	1	6	5	8	7	10	9
4	3	4	5	1	0	2	9	10	11	6	7
5	4	5	3	6	2	0	1	11	10	12	8
6	6	7	8	5	9	1	0	2	3	4	13
7	7	6	9	8	10	11	2	0	1	3	4
8	8	9	6	7	11	10	3	1	0	2	5
9	9	8	7	10	6	12	4	3	2	0	1
10	10	11	12	9	7	8	13	4	5	1	0

Table 1. Part of the multiplication table of Q_5.

gives the first few entries of the multiplication table of Q_5.

Seeding with 0, one obtains Q_0 as a countable elementary abelian 2-group. In the theory of combinatorial games, the multiplication of Q_0 is known as *nim sum* [5]. Greedy quasigroups will be seen as a generalization of nim. Each position X in the game of nim is assigned a natural number value x, and the nim sum $x \oplus y$ denotes the value of the nim position $X + Y$ obtained by juxtaposing X with a second position Y of value y. Seeding with 1, the quasigroup Q_1 gives a comparable description of the juxtaposition of positions in the game of misère nim – nim played to lose. Section

discusses elementary properties of the greedy quasigroups: commutativity, associativity, total symmetry, and the existence of identity, idempotent, and nilpotent elements. The next two sections (which may be skipped at first reading) comprise a number of technical lemmas about the multiplication by 2 and 3 in Q_s for $s > 0$. These lemmas drive the theorems regarding the multiplication groups in Section . Section examines the subquasigroup structure of the greedy quasigroups. It transpires that while Q_0, Q_1 have uncountably many subquasigroups, Q_2 has just one proper, non-trivial subquasigroup, and Q_s has none for $s > 2$ (Theorem 6.2). It is also shown that for $s > 2$, the quasigroup Q_s is simple. The congruences of Q_0 correspond directly to its subgroups, essentially forming a projective geometry of countable dimension over the 2-element field. For $s > 1$, the greedy quasigroups Q_s are shown to be simple in Theorem 6.3. Section considers homomorphisms between greedy quasigroups. It is shown that the greedy quasigroups are mutually non-isomorphic (Theorem 7.1), and indeed that for distinct positive seeds s, t, the only homomorphism from Q_s to Q_t is the constant map taking the value 1 (Theorem 7.11). Finally, Theorem 7.12 shows that for $s > 2$, the only endomorphisms of Q_s are the constant and the identity. In particular, Q_s is *rigid* in the sense of having a trivial automorphism group. It may be worth noting that the properties of the greedy quasigroups Q_s for $s > 2$, namely simplicity, rigidity, and lack of proper, non-trivial subalgebras, are reminiscent of the Foster-Pixley characterization of (necessarily finite) primal algebras [7]. The paper concludes with a brief characterization of greedy quasigroups in terms of combinatorial game theory. For algebraic concepts and conventions that are not otherwise explained here, especially involving quasigroups, readers are referred to [8]. Note that mappings are usually placed to the right of their arguments, allowing composition in natural order, and minimizing the number of brackets that otherwise proliferate in the study of non-associative structures such as quasigroups.

2. Elementary properties

Recall that a quasigroup $(Q, \cdot, /, \backslash)$ is said to be *commutative* or *associative* respectively if its multiplication $\cdot$ is commutative or associative.

Proposition 2.1. *For each seed s, the quasigroup Q_s is commutative.*

Proof. By induction, using (2):

$$\begin{aligned} l \cdot m &= \operatorname{mex}(\{i \cdot m \mid i < l\} \cup \{l \cdot j \mid j < m\}) \\ &= \operatorname{mex}(\{m \cdot i \mid i < l\} \cup \{j \cdot l \mid j < m\}) \\ &= \operatorname{mex}(\{i \cdot l \mid i < m\} \cup \{m \cdot j \mid j < l\}) = m \cdot l. \end{aligned}$$

(The induction hypothesis is used for the second equality.) □

Proposition 2.2. *Suppose* $s > 0$.

1. $\forall\ 0 < x \leqslant s,\ 0 \cdot x = x \cdot 0 = x - 1.$
2. $\forall\ x > s,\ 0 \cdot x = x \cdot 0 = x.$
3. $\forall\ 0 \leqslant x \leqslant s,\ 1 \cdot x = x \cdot 1 = x.$

Proof. (1) Since $0 \cdot 0 = s$, $1 \cdot 0 = 0$, and applying (2) to each successive term, one has $x \cdot 0 = \operatorname{mex}\{s, 0, 1, \ldots, (x-1) \cdot 0 = (x-2)\} = x - 1$.

(2) For $x = s+1$, (2) gives $0 \cdot x = \operatorname{mex}\{s, 0, 1, \ldots, s-1\} = s+1$. Then $0 \cdot x = x$ for $x > s$ by induction.

(3) Note $0 \cdot 1 = 0$. Then for $x \leqslant s$, induction yields

$$x \cdot 1 = \operatorname{mex}\{0, 1, \ldots, x-1, 0 \cdot x = x - 1\} = x. \qquad \square$$

Corollary 2.3. *For* $s > 0$, *the quasigroup* Q_s *is not associative.*

Proof. $(0 \cdot 0) \cdot (s+1) = s \cdot (s+1) \neq 0 \cdot (s+1) = 0 \cdot (0 \cdot (s+1))$. □

Definition 2.4. The *hub* of a greedy quasigroup Q_s is defined to be the subset $H_s = \{0, \ldots, s\}$.

In Table 1, the hub H_5 is marked off by separating lines.

Remark 2.5. The element 0 is the identity element of the group Q_0. For $s > 0$, the quasigroup Q_s does not have a universal identity element. However, the later parts of Proposition 2.2 may be interpreted as saying that 1 is an identity for the hub, while 0 is an identity outside the hub. In particular, 1 is the only idempotent element of Q_s, i.e., the only element x forming a singleton subquasigroup $\{x\}$.

A quasigroup $(Q, \cdot, /, \backslash)$ is said to be *totally symmetric* if its three binary operations agree, i.e., if the implication

$$x_1 \cdot x_2 = x_3 \Rightarrow x_{1\pi} \cdot x_{2\pi} = x_{3\pi} \tag{3}$$

holds for all permutations π of the index set $\{1,2,3\}$. (Commutativity means that (3) holds for $\pi = (12)$.) Note that Q_0, like any elementary abelian 2-group, is totally symmetric. Now outside the hub, the multiplication on Q_1 is constructed exactly as in Q_0. Furthermore, the hub of Q_1 is totally symmetric, being isomorphic to the subgroup $\{0,1\}$ of Q_0. Thus Q_1 is also totally symmetric.

Lemma 2.6. *Suppose $s > 0$. For $x > s$,*

$$x \cdot 1 = \begin{cases} x+1, & x - s \equiv_2 1 \\ x-1, & x - s \equiv_2 0. \end{cases}$$

Proof. As an induction basis, note:

$$(s+1) \cdot 1 = \operatorname{mex}\{0, 1, \ldots, s, (s+1) \cdot 0 = s+1\} = s+2;$$
$$(s+2) \cdot 1 = \operatorname{mex}\{0, 1, \ldots, s, s+2, (s+2) \cdot 0\} = s+1.$$

Consider $x > s$. By induction, for $x - s \equiv_2 1$,

$$x \cdot 1 = \operatorname{mex}\{0, 1, \ldots, x-1, x \cdot 0\} = x+1,$$

and for $x - s \equiv_2 0$,

$$x \cdot 1 = \operatorname{mex}\{0, 1, 2, \ldots, x-3+1, x-2-1, x-1+1, x \cdot 0\} = x-1. \quad \square$$

Recall that in any quasigroup $(Q, \cdot, /, \backslash)$, the *square* x^2 of an element x is $x \cdot x$. An element of a greedy quasigroup is described as *nilpotent* if its square is 0. All but at most two elements of a greedy quasigroup are nilpotent, and 0 is the only square of infinitely many elements.

Theorem 2.7. *For $x > 1$ in any greedy quasigroup, $x^2 = 0$.*

Proof. The result is immediate in Q_0, so suppose $s > 0$. Recall $0 \cdot 1 = 0 = 1 \cdot 0$. Thus the first place 0 can appear in the 2-column of the Latin square is the 2-row, so it must appear there. Then the first place 0 can and must appear in the 3-column is the 3-row. Fill in the first n columns (labelled $0, \ldots, n-1$) by induction. The first place 0 can appear in the n-column is in the n-row. Thus by induction $n \cdot n = 0$ for all $n > 1$. $\square$

Corollary 2.8. *Consider the greedy quasigroup Q_s.*

1. *If $s = 1$, then $0^2 = 1^2 = 1$.*
2. *For $s \neq 1$, the element 0 is the only square of more than one element.*

3. Multiplication by 2

Throughout the next two technical sections, which may be skipped at first reading, assume $s > 0$. (Later, it will be implicitly necessary to assume that s is "sufficiently large.") Consider the inductive construction of the Latin square that forms the body of the multiplication table of Q_s. There is a critical dependence on the congruence class of the seed to certain moduli. A column is said to be *complete at entry* n if its first $n+1$ elements are precisely the numbers $0, 1, \ldots, n$. The proofs are by induction and can be done by hand in a similar fashion to those above.

Lemma 3.1. *For* $x < s$,

$$x \cdot 2 = \begin{cases} x+1, & x \equiv_3 0, 1; \\ x-2, & x \equiv_3 2. \end{cases}$$

The post-hub behavior of the 2-column depends on the congruence class of the seed modulo 3. We consider each class in turn.

Lemma 3.2. *For* $s \equiv_3 0$ *and* $s \equiv_3 1$ *and* $x > s+1$:

$$x \cdot 2 = \begin{cases} x+1, & x - s \equiv_2 0; \\ x-1, & x - s \equiv_2 1. \end{cases}$$

Lemma 3.3. *For* $s \equiv_3 2$, *and* $x > s$,

$$x \cdot 2 = \begin{cases} x+2, & x - s \equiv_4 1, 2; \\ x-2, & x - s \equiv_4 3, 0. \end{cases}$$

4. Multiplication by 3

Multiplication by 3 is the last detailed case that is analyzed in this paper. Its structure is slightly more difficult than in the earlier cases. For each of the following lemmas, suppose that the seed is sufficiently large. The first lemma collects some preliminary calculations.

Lemma 4.1. $0 \cdot 3 = 2$, $1 \cdot 3 = 3$, $2 \cdot 3 = 4$, $3 \cdot 3 = 0$, $4 \cdot 3 = 1$.

Lemma 4.2. *For* $5 \leqslant x \leqslant s$:

$$x \cdot 3 = \begin{cases} x+1, & x \equiv_9 5, 8; \\ x+2, & x \equiv_9 6, 1, 2; \\ x-2, & x \equiv_9 7, 0, 4; \\ x-1, & x \equiv_9 3. \end{cases}$$

After each ninth step, the column becomes complete.

In the remainder of this section, only the 3-column of the multiplication table for $s \equiv_3 2$ is considered, since this is the only case needed for the subsequent results. Note that $s \equiv_9 2, 5, 8$. Each case yields a different pattern after the row labelled by the seed.

Lemma 4.3. *For* $x > s \equiv_9 2$:

$$x \cdot 3 = \begin{cases} x-2, & x-s \equiv_4 1, 2; \\ x+2, & x-s \equiv_4 3, 0. \end{cases}$$

Lemma 4.4. *For* $x > s \equiv_9 5$:

$$x \cdot 3 = \begin{cases} x-1, & x-s \equiv_2 1; \\ x+1, & x-s \equiv_2 0. \end{cases}$$

Lemma 4.5. *For* $s \equiv_9 8$, $(s+1) \cdot 3 = s-1$. *For* $x \geqslant s+2$:

$$x \cdot 3 = \begin{cases} x+1, & x-s \equiv_2 0; \\ x-1, & x-s \equiv_2 1. \end{cases}$$

5. Multiplication groups

In this section, the multiplication groups for each Q_s are analyzed. The analysis yields easy proofs of some later theorems.

Consider

$$G = \langle R(0), R(1), R(2) \rangle < \mathrm{Mlt}(Q_s).$$

$$R(0) = (0, s, s-1, s-2, \ldots, 1)$$
$$R(1) = (s+1, s+2)(s+3, s+4)\ldots(s+2n+1, s+2n+2)\ldots$$
$$R(2) = (0, 2, 1)(3, 5, 4)\ldots$$

But one has to consider the seed mod 3.

- For $s \equiv_3 0$, one has $(0,2,1)\dots(s{-}3, s{-}1, s{-}2){\cdot}(s, s{+}1)(s{+}2, s{+}3)\dots$
- For $s \equiv_3 1$, one has $(0,2,1)\dots(s, s+1, s-1)\cdot(s+2, s+3)\dots$
- For $s \equiv_3 2$, one has $(0,2,1)\dots(s-1, s, s-2)\cdot(s+1, s+3)(s+2, s+4)(s+5, s+7)(s+6, s+8)\dots$

Consider $R(0), R(1), R(2)$ in $S_{\mathbb{N}}$. A natural question is whether or not the groups

$$G = \langle R(0), R(1), R(2)\rangle$$

and

$$F = \langle R(0), R(1), R(2), R(3)\rangle$$

have transitive actions on Q_s. If so, are the groups multiply transitive?

5.1. Transitivity

Lemma 5.1. *For all s, $\langle R(0)\rangle$ acts transitively on the hub.*

Proof. By Lemma 2.2, $0 \cdot x = x - 1$ for $0 < x \leqslant s$ and $0 \cdot 0 = s$. Thus $xR(0)^x = 0$, and $0R(0)^{y+1} = s - y$. Therefore for $x, z = s - y \in H$, there is an n such that $xR(0)^n = z$. □

Lemma 5.2. *For $s \equiv_3 0, 1$, $Q_s \setminus H_s$ is in one orbit of the action of G on Q_s. Moreover, one can choose $g \in G$ so that $x_1 g = x_2$ for any $x_1, x_2 \in Q_s \setminus H_s$ and g stabilizes 1.*

Proof. Let $x = s+2n-i$, $y = s+2m-j$, where $n, m \in \mathbb{N}$ and $i, j \in \{0,1\}$. Let $\tau = R(1)^i(R(2)R(1))^{m-n}R(1)^j$. Now it is shown that $x\tau = y$. The initial multiplication by $R(1)^i$ sends both $s + 2n - i$ to $s + 2n$. Now by Lemmas 2.6 and 3.1 an application of $R(2)R(1)$ sends $s+2n$ to $s+2n+2$. So $(R(2)R(1))^t$ sends $s + 2n$ to $s + 2n + 2t$. Therefore $R(1)^i(R(2)R(1))^t$ sends $s+2n-i$ to $s+2n+2t$. Finally $R(1)^j$ sends this to to $s+2n+2t-j$. Therefore $(s+2n-i)\tau = s+2n+2(m-n)-j = s+2m-j$. To stabilize 1, use $\sigma = R(1)^i R_1(2,0)^{m-n}R(1)^j$. Note that since $R_1(2,0) = R(2)R(0)R(1)^{-1}$, on $Q_s \setminus H_s$, $R_1(2,0)$ behaves like $R(2)R(1)$, since $xR(0) = x$ and $xR(1)^2 = x$ for $x \in Q_s \setminus H_s$. Thus $x\sigma = xR(1)^i(R(2)R(1))^{n-m}R(1)^j = y$ as above. □

Theorem 5.3. *The group G acts transitively on Q_s for $s \equiv_3 0, 1$.*

Proof. Using Lemmas 5.1 and 5.2, it remains to show that a hub element can be sent to a non-hub element. Note that $s \cdot 2 = s + 1$ in this case. So to send a hub element h to a non-hub element $s + 2n - j$, use $\sigma = R(0)^{h+1}R(2)R(1)\,(R(2)R(1))^{n-1}\,R(1)^j$. □

For $s \equiv_3 2$ the situation is more complex.

Lemma 5.4. *Let $\sigma_{k,i} = R(2)^k R(1)^i$ for $k, i \in \{0, 1\}$. Then in Q_s for $s \equiv_3 2$, $\sigma_{k,i}$ sends $s + 4n - 2k - i$ to $s + 4n$.*

Proof. Since multiplication by 2 adds or subtracts 2, $R(2)^k$ sends $s + 4n - 2k - i$ to $s + 4n - i$. Now multiplication by 1 adds or subtracts 1. So $R(1)^i$ sends $s + 4n - i$ to $s + 4n$. □

Lemma 5.5. *For $s \equiv_9 5, 8$, $\tau = R(3)R(2)R(1)$ sends $s + 4n$ to $s + 4n + 4$.*

Proof. First, $(s + 4n)R(3) = s + 4n + 1$ by Lemmas 4.4 and 4.5. Then $(s+4n+1)R(2) = s+4n+3$ by Lemma 3.3 and $(s+4n+3)R(1) = s+4n+4$ by Lemma 2.6. Thus $(4n)\tau = (4n)R(3)R(2)R(1) = 4n + 4$. □

Lemma 5.6. *For $s \equiv_9, 2$ $\tau = R(3)R(2)$ sends sends $s + 4n$ to $s + 4n + 4$*

Proof. First $(s + 4n)R(3) = (s + 4n + 2)$ by Lemma 4.3. Then $(s + 4n)$ $(R(3)R(2)) = s + 4n + 4$ by Lemma 3.3. □

Lemma 5.7. *For $s \equiv_3 2$, $Q_s \setminus H_s$ is in one orbit of the action of G on Q_s. Moreover, one can choose $g \in G$ so that $x_1 g = x_2$ for any $x_1, x_2 \in Q_s \setminus H_s$ and g stabilizes 1.*

Proof. We show that any $x \in Q_s \setminus H_s$ can be sent to $y \in Q_s \setminus H_s$. Let $x = 4n - 2k - i$ and $y = 4m - 2k' - i'$, where $k, k', i,' i \in \{0, 1\}$. Then for $\varphi = \sigma_{k,i}\tau^{m-n}\sigma k', i'^{-1}$, $x\varphi = y$:

$$\begin{aligned}(s + 4n - 2k - i)\varphi &= (s + 4n - 2k - i)\sigma_{k,i}\tau^{m-n}\sigma_{k',i'} \\ &= (s + 4n)\tau^{m-n}\sigma_{k',i'} \\ &= (s + 4m)\sigma_{k',i'} \\ &= s + 4m - k' - i'\end{aligned}$$

Thus $x\varphi = y$. Note that outside the hub $R(0)$ stabilizes x. So $\alpha = R_1(3, 0)R_1(2, 0)R(1)$ behaves like $R(3)$ and stabilizes 1 while $\beta = R_1(2, 0)R(1)$ behaves like $R(2)$ and stabilizes 1. Now apply Lemma 5.7 with α in place of $R(3)$ and β in place of $R(2)$ □

Theorem 5.8. *For $s \equiv_3 2$, F acts transitively on Q_s.*

Proof. It remains to be shown that one can send a hub element to a non-hub element as before. Let $h \in H_s$ and $x = s + 4n - 2k - i$. First, let $\psi = R(0)^{h+1}R(3)\sigma_{1,1}\tau^{n-1}\sigma_{k,i}$. Then $h\psi = x$ by the above lemmas. □

5.2. 2-transitivity

The goal of this section is to prove that $Mlt(Q_s)$ is 2-transitive.

Lemma 5.9. *Let $H = \langle R(0), R(2)\rangle$. Then H_s is in one orbital of the action of H on Q_s for $s \equiv_3 0, 1$.*

Proof. Given $h_1, h_2, x_1, x_2 \in H_s$, there is an n so that $h_1R(0)^n = s$ (by Lemma 5.1). So $h_1R(0)^nR(2) = s + 1$. Let $h_2R(0)^nR(2) = k$. Now choose m so that $kR(0)^m = x_2R(0)^{-(s-x_1)}R(2)^{-1}$. Thus $h_1\sigma = x_1$ and $h_2\sigma = x_2$ for $\sigma = R(0)^nR(2)R(0)^mR(2)^{-1}R(0)^{s-x_1}$. □

Lemma 5.10. *Let $H = \langle R(0), R(3)\rangle$. Then H_s is in one orbital of the action of H on Q_s for $s \equiv_3 2$.*

Proof. Given $h_1, h_2, x_1, x_2 \in H_s$, there is an n so that $h_1R(0)^n = s$ (by Lemma 5.1). So $h_1R(0)^nR(3) = s + 1$. Let $h_2R(0)^nR(3) = k$. Now choose m so that $kR(0)^m = x_2R(0)^{-(s-x_1)}R(3)$. Thus $h_1\sigma = x_1$ and $h_2\sigma = x_2$ for $\sigma = R(0)^nR(3)R(0)^mR(3)^{-1}R(0)^{s-x_1}$. □

Remark 5.11. The above two lemmas, along with the fact that $hR(1) = h\ \forall h \in H_s$ show that the hub is in one orbital of the action of F.

Lemma 5.12. *For $x_1 \in Q_s \setminus H_s$ and h_1, h_2, h_3 there is a σ so that $x_1\sigma = h_2$ and $h_1\sigma = h_3$.*

Proof. Use $R(0)^n$ for some n so send h_1 to 1. By Lemmas 5.2 and 5.7, there is a β so that $1\beta = 1$ and $x_1\beta = s+1$. Then for $s \equiv_3 0, 1$ $\gamma = R(0)^n\beta R(2)^{-1}$ is such that $x_1\gamma, h_1\gamma \in H_s$. For $s \equiv_3 2$ use $\gamma = R(0)^n\beta R(3)^{-1}$. Now since H_s is in one orbital of the action of $\langle R(0), R(2), R(3)\rangle$ (Remark 5.11), the proof is complete. □

Lemma 5.13. *For $x_1, x_2 \in Q_s \setminus H_s$ and $h_1, h_2 \in H_s$, there is a σ so that $x_i\sigma = h_i$.*

Proof. Let α be so that $x_1\alpha = 1$. Then perhaps $x_2\alpha = h \in H_s$. Then by Lemma 5.9, there is a β, so that $1\beta = h_1, h\beta = h_2$. Thus $\sigma = \alpha\beta$. If $x_2\alpha = x \notin H_s$ apply Lemma 5.12. □

Theorem 5.14. *F acts 2-transitively on Q_s.*

Proof. We find a σ that sends $(x_1, x_2) \in Q_s^2$ to (y_1, y_2). First by the above three lemmas, there is a map α so that $(x_1, x_2)\alpha = (0, 1)$, and a map β so that $(y_1, y_2)\beta = (0, 1)$. Then $(x_1, x_2)\alpha\beta^{-1} = (y_1, y_2)$ □

5.3. High transitivity

It has been shown how to construct permutations in $F \leqslant \mathrm{Mlt}(Q_s)$ that are 2-transitive. The question is whether one can go farther.

First note that since F is 2-transitive it is primitive (Lemma 4.10 in [3]). Therefore we can apply Lemma 10.8 in [3] with the hub as the Jordan set. This theorem says that if a permutation group on Ω is primitive on an infinite set with a subgroup H that is transitive on a set, X, and fixes the complement of X, the multiplication group is highly transitive. Moreover, if X is finite, $\mathrm{Alt}(\Omega) \leqslant F$. Thus $\mathrm{Alt}(\mathbb{N}) \leqslant F \leqslant \mathrm{Mlt}(Q_s)$.

6. Subquasigroups

As noted in Remark 2.5, each greedy quasigroup has a unique singleton subquasigroup: $\{0\}$ in the elementary 2-group Q_0, and $\{1\}$ in Q_s for $s > 0$. We refer to the singleton subquasigroup and the empty subquasigroup as the *trivial* subquasigroups of the greedy quasigroups. The group Q_0 has uncountably many subquasigroups, since for each of the uncountably many subsets S of $\mathbb{N}$, the vector

$$(0\chi_S, 1\chi_S, \dots, n\chi_S, \dots) \tag{4}$$

of values of the characteristic function of S generates a distinct subgroup of the isomorphic copy $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ of Q_0.

Proposition 6.1. *The greedy quasigroup Q_1 has uncountably many subquasigroups.*

Proof. Outside the hub $\{0, 1\}$, the multiplication on Q_1 is constructed exactly as in Q_0. Thus for each subgroup P of Q_0 with $\{0, 1\} \leqslant P$, the subset P of $\mathbb{N}$ forms a subquasigroup of Q_1. But Q_0 has uncountably many such subgroups P. □

The respective hubs H_1 and H_2 of Q_1 and Q_2 form cyclic groups, with 1 as the identity element (Remark 2.5). These cases are exceptional.

Proposition 6.2. *For $s > 2$, there are no non-trivial subquasigroups of Q_s.*

Proof. Note that F is transitive for all $s \geqslant 3$. Thus if a subquasigroup, H, contains $0, 1, 2, 3$ then $H = Q_s$. Let H be a subquasigroup. If $0 \in H$, then $H_s \subset H$. In particular for $s \geqslant 3$, $0, 1, 2, 3 \in H$ and $H = Q_s$. Suppose $x \neq 0, 1 \in H$, then $x \cdot x = 0 \in H$, so as above $H = Q_s$. Thus the only subquasigroup is the trivial subquasigroup $\{1\}$. □

Proposition 6.3. *For $s \geqslant 2$, Q_s is simple.*

Proof. This follows immediately since $\mathrm{Mlt}(Q_s)$ is 2-transitive. □

7. Homomorphisms

Theorem 7.1. *For $i \neq j$, $Q_i \ncong Q_j$.*

Proof. In both Q_i, Q_j, 0 is the unique element that fixes infinitely many elements. So for any isomorphism φ, $\varphi : 0 \mapsto 0$. In $\mathrm{Mlt}(Q_i)$, $R(0)$ is an $i+1$-cycle, but in Q_j $R(0)$ is a $j+1$-cycle. Thus $Q_i \ncong Q_j$. □

One can actually prove stronger results.

Lemma 7.2. *Let $\varphi : Q_i \to Q_j$.*

(*a*) *If φ is injective then there is a $k \in Q_i$ such that $k, k\varphi$ are both nilpotent.*

(*b*) *If φ is surjective then there is a $k \in Q_i$ such that $k, k\varphi$ are both nilpotent.*

Proof. There are only two elements $k \in Q_i$ such that $k \cdot k \neq 0$, namely $0, 1$, and similarly for Q_j.

(*a*) Let φ be injective. Suppose that $x\varphi, y\varphi$ are not nilpotent. Let z be nilpotent, then $z\varphi$ is not $x\varphi, y\varphi$ and these are the only non-nilpotent elements in Q_j. Thus both $z, z\varphi$ are nilpotent.

(*b*) Since φ is surjective, at most two of the nilpotent elements of Q_j can be the image of non-nilpotent elements of Q_i. There must be nilpotent elements on Q_i that are mapped to nilpotent elements of Q_j.

□

In what follows, the notations q_i, q_j are used for an element $q \in Q_i$ to distinguish it from $q \in Q_j$.

Lemma 7.3. *Let $\varphi : Q_i \to Q_j$ be a homomorphism and $0_i\varphi = 0_j$. If $x \cdot x = 0$, then $x\varphi \cdot x\varphi = 0$.*

Proof. $0_j = 0_i\varphi = (x \cdot x)\varphi = x\varphi \cdot x\varphi$. □

Lemma 7.4. *Let $\varphi : Q_i \to Q_j$ be a homomorphism. If there is an element $x \in Q_i$ such that $x \cdot x = 0$ and $x\varphi \cdot x\varphi = 0$, then $0_i\varphi = 0_j$.*

Proof. Let k be one such element. Then $0_j = 0_i\varphi = (k \cdot k)\varphi = k\varphi \cdot k\varphi$. □

Remark 7.5. In particular, Lemma 7.3 and Lemma 7.4 are true for surjective and injective homomorphisms.

Lemma 7.6. *For any homomorphism $\varphi : Q_i \to Q_j$ and $i, j \neq 0, 1$, $1_i\varphi = 1_j$.*

Proof. This follows from the fact that 1_i is the only idempotent element of Q_i. (Everything else other than 0_i is nilpotent). □

Lemma 7.7. *For any surjective (injective) homomorphism $\varphi : Q_i \to Q_j$, $s_i\varphi = s_j$.*

Proof. $s_i\varphi = (0_i \cdot_i 0_i)\varphi = 0_i\varphi \cdot_j 0_i\varphi = 0_j \cdot_j 0_j = s_j$. □

Remark 7.8. In fact, this is true if $0_i\varphi = 0_j$.

Theorem 7.9 (Homomorphism Theorem). *Suppose $i, j > 1$.*

(*a*) *There is no injective homomorphism $\varphi : Q_i \to Q_j$.*

(*b*) *There is no surjective homomorphism $\varphi : Q_i \to Q_j$.*

Proof. Note that by looking at the multiplication table for Q_j, that $s_jL(0_j)^{s_j} = s_j$ and $s_jL(0_i)^i \neq s_j$ for $i < s_j$. Since $s_i\varphi = s_j$, then $s_j = s_i\varphi = s_iR(0_i)^i = s_i\varphi R(0_i\varphi)^i = s_jR(0_j)^i$. Thus $j + 1 | i + 1$. Perhaps one can "loop" several times, but the loop must be completed. Thus there is no injective or surjective homomorphism $\varphi : Q_i \to Q_j$, if $i < j$. So, suppose that $j + 1 | i + 1$, but $j \neq i$. Note that $s_iR(0)^{j-1}$ is nilpotent. Then $s_iR(0)^{j-1}\varphi = s_i\varphi R(0\varphi)^{j-1} = s_jR(0_j)^{j-1} = 1_j$. This is contradicts Lemma 7.3, since a nilpotent must be mapped to a nilpotent and 1_j is idempotent. □

Remark 7.10. Theorem 7.1 can be seen as a corollary to the Homomorphism Theorem.

Not only are the Q_i's are not isomorphic, there is no injective or surjective homomorphism between them. It is natural to ask whether there is any non-trivial homomorphism between them. Of course, there is the trivial homomorphism $x\varphi = 1, \forall x \in Q_i$ for any Q_i, Q_j. It turns out that this is the only homomorphism $\varphi : Q_i \to Q_j$ for $i \neq j$.

Theorem 7.11. *The only homomorphism $\varphi : Q_i \to Q_j$ for $i \neq j$ is the trivial homomorphism.*

Proof. Let $\varphi : Q_i \to Q_j$. If there is a nilpotent element x such that $x\varphi$ is also nilpotent, by Lemma 7.4 $0_i\varphi = 0_j$, so then by Lemma 7.7 $s_i\varphi = s_j$. Then the homomorphism fails as in Theorem 7.9. Thus for any nilpotent x, $x\varphi$ is either 0 or 1. If $x \neq 0$ and $x\varphi = 0$, then $0\varphi = (x \cdot x)\varphi = x\varphi x\varphi = 0_j \cdot 0_j = s_j$. Then for any nilpotent y, $s_j = 0\varphi = (y \cdot y)\varphi = y\varphi \cdot y\varphi$. So s_j is the square of $y\varphi$. Thus $y\varphi = 0_j$ for any nilpotent y. Now, $s_i\varphi = (0_i \cdot 0_i)\varphi = 0_i\varphi 0_i\varphi = s_j \cdot s_j = 0_j$. However, in any Q_i there are nilpotent elements x, y such that $xy = s_i$. Then $s_i\varphi = (xy)\varphi = x\varphi y\varphi = 0_j \cdot 0_j = s_j$. This is a contradiction, so there is no x so that $x\varphi = 0_j$. Thus $x\varphi = 1_j$ for all nilpotent x. In particular $s_i\varphi = 1$, so $0_i\varphi = (s_i \cdot s_i)\varphi = s_i\varphi \cdot s_i\varphi = 1_j \cdot 1_j = 1$. Thus φ is trivial. □

Theorem 7.12. *For $s > 2$, there are only two endomorphisms of Q_s, the constant and the identity. In particular, Q_s is rigid.*

Proof. Suppose that $f : Q_s \to Q_s$ is an endomorphism. Since Q_s is simple by Theorem 6.3, the kernel congruence of f is either trivial (the equality relation) or improper. If it is improper, then f is constant, its image being the unique singleton subquasigroup $\{1\}$ of Q_s. Otherwise, f injects. Now 0 is the only element that is the square of more than one element, so $0f = 0$. The image $sf = (0 \cdot 0)f = 0^f \cdot 0^f$ of the seed is a square, namely $1, 0$ or s. If $sf = 1$, then $0^f \cdot 0^f = 1$, yielding the contradiction $0f = 1$. Again, $sf = 0$ would contradict the injectivity of f. Thus $sf = s$. By Lemma 5.2, $s - r = sR(0)^r$ for $0 \leqslant r < s$. Then $(s - r)f = sR(0)^r f = sR(0)^r = s - r$, so the hub is fixed. Since the hub generates all of Q_s, it follows that Q_s is fixed, and f is the identity. □

8. Game theory applications

Greedy quasigroups are motivated in part by combinatorial games, in particular by nim. Nim is a game played with several piles, or heaps of counters. A player selects a pile and removes some, or possibly all the counters in the pile. The player to make the last move wins. With only two piles, the strategy is simple: equalize the piles, and then when your opponent removes n counters from one pile, remove n from the other. In this way, a player will never be at a loss for a move. With three or more non-empty piles, the strategy is a little more elusive. One must compute the *nim-sum*. The nim-sum is a way of reducing a collection of piles to a single value. This value represents the size of a single pile that is equivalent to the original position. If this pile were included in the original position, the resulting game would be a win for the first player. For details, see [1]. An alternative characterization of nim is that of a Rook on a quarter-infinite chessboard. Place a Rook on the board and make legal Rook moves up and left of the board. A player wins by placing the Rook on the upper-left corner. Now, greedy quasigroups have the following characterization as a game: place a nim-heap of size n, $n \geqslant 0$ on a chessboard. Move the heap as a Rook. Once the heap reaches the upper-left square, players may play in the nim heap. Clearly, with a single non-empty nim-heap on the board, one can win by forcing the other player to place the heap on the upper-left square and then removing the entire nim-heap. These game are examples of the sequential compounds in [9]. The difficulty arises when several heaps of different sizes are placed on the board. To play correctly, one must compute the value of each heap, with is a function of its size and its location. In this way, one can compute the nim-value of the position, and using combinatorial game theory, make the correct move. Suppose heaps of sizes $n_1, n_2, \ldots, n_k$ at locations $(x_1, y_1), \ldots, (x_n, y_n)$. The value of each heap is $x_i \cdot_i y_i$ where $\cdot_i$ is the multiplication in Q_{n_i}. The total value of the game is then:

$$\bigoplus_{i=1}^{k} x_i \cdot y_i$$

where $\oplus$ is nim-addition. A natural generalization is to place an entire game of nim on a square. This does not produce any new games, since each game of nim is equivalent to a single nim heap; so one might as well simply put the single nim-heap on the square.

References

[1] **E. Berlekamp, J. H. Conway and R. K. Guy:** *Winning Ways for your Mathematical Plays*, A K Peters, Ltd, 2001.

[2] **E. Berlekamp, J. H. Conway and R. K. Guy:** *Winning Ways for your Mathematical Plays*, A K Peters, Ltd, 2002.

[3] **M. Bhattacharjee et. al.:** *Notes on Infinite Permutation Groups*, Lecture Notes in Mathematics, 1998.

[4] **G. Birkhoff:** *Lattice Theory*, American Mathematical Society, 1967.

[5] **J. H. Conway:** *On Numbers and Games*, A K Peters, Ltd, 2002.

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

[7] **A. L. Foster and A. F. Pixley:** *Semi-categorical algebras I: semi-primal algebras*, Math. Z. **83** (1964), 147 – 169.

[8] **J. D. H. Smith and A. B. Romanowska:** *Post-Modern Algebra*, Wiley, 1999.

[9] **W. Stromquist and D. Ullman:** *Sequential compounds of combinatorial games*, Theoretical Computer Science **(119)** (1993), 311 – 321.

Iowa State University
Department of Mathematics
Ames, IA 50011
USA
E-mail: tarice@iastate.edu

Received November 2, 2006