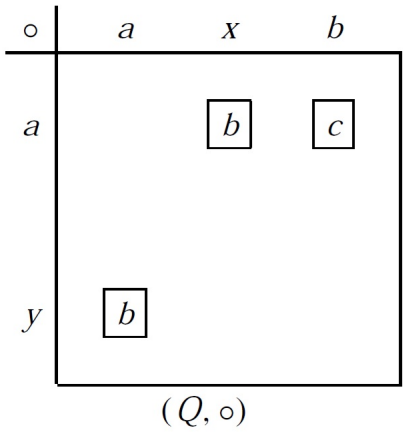
Chapter 3. Quasigroup Identities and Graph Decompositions

Note. In this chapter, we consider identities in quasigroups in Section 3.1, apply these identities to Mendelsohn triple systems in Section 3.2, and apply these identities to Steiner triple systems in Section 3.3.

3.1. Quasigroup Identities

Note. In this section, we introduce an orthogonal array associated with a quasigroup. We then relate identities in the quasigroup to permutations of the rows of the orthogonal array. In the process, we must discuss a little bit of group theory from modern algebra.

Note 3.1.A. Let $(Q, \circ)$ be a quasigroup of order n and define array R as an $n^2 \times 3$ array where $((a, b), c) := (a, b, c) \in R$ if and only if $a \circ b = c$. Since $a \circ x = b$ and $y \circ a = b$ have unique solutions for all $a, b \in Q$, then we have the following occurring exactly once: (1) a in the first entry and b in the second entry (namely, when the third entry is c), (2) a in the first entry and b in the third entry (namely when the second entry is the unique x such that $a \circ x = b$), and (3) a in the second entry and b in the third entry (namely when the first entry is the unique y such that $y \circ a = b$). As Linder and Rodger put it (see page 65) "if we run our fingers down any two columns of R we obtain all n^2 ordered pairs $(a, b) \in Q \times Q$," as illustrated below.



$R =$

a	b	c
a	x	b
y	a	b

Note. The converse of the claim in Note 3.1.A also holds. We formally claim this in the following lemma.

Lemma 3.1.A. Let R be an $n^2 \times 3$ with the property that each ordered pair (a, b) satisfies the following: (1) a in the first column and b in the second column in exactly once (say when c is in the third column), (2) a in the first column and b in the third column exactly once (say when x is in the second column), and (3) a in the second column and b in the third column in exactly once (say when y is in row one). Define $a \circ b = c$ based on property (1). Then $(Q, \circ)$ is a quasigroup.

Note/Definition. We now have that every quasigroup $(Q, \circ)$ is equivalent to an $n^2 \times 3$ array R (called an *orthogonal array*) such that $a \circ b = c$ if and only if $((a, b), c) := (a, b, c) \in R$. We now illustrate this idea with a quasigroup Q and an orthogonal array R.

Example 3.1.1. Consider the (idempotent) quasigroup on the left (below). Then the corresponding orthogonal array R is as follows:

$(Q, \circ) =$

$\circ$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

$R =$

1	1	1
1	2	3
1	3	4
1	4	2
2	1	4
2	2	2
2	3	1
2	4	3
3	1	2
3	2	4
3	3	3
3	4	1
4	1	3
4	2	1
4	3	2
4	4	4

Note 3.1.B. Recall from Introduction to Modern Algebra (MATH 4127/5127; see my online notes on Section II.8. Groups of Permutations) that the symmetric group S_3 has the following six elements. Here, the symbols 1, 2, or 3 in the first row of each matrix are mapped to the symbols 1, 2, or 3 in the second row and same

column of each matrix. The "cycle notation" is also given

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3) \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2,3)$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3) \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (2)(1,3)$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2) \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)(3)$$

Under composition of mappings as a group operation, we have the following multiplication table (or "Cayley table"):

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Notice that this table results from multiplying the permutations from *right* to *left*. We have that S_3 is not commutative because $\rho_2\mu_1 = \mu_3 \neq \mu_2 = \mu_1\rho_2$. In fact, this is the smallest order noncommutative (or nonabelian) group.

Definition. For R an $n^2 \times 3$ orthogonal array and $\alpha \in S_3$ a permutation on $\{1,2,3\}$, define $R\alpha$ to be the $n^2 \times 3$ array obtained from R by permuting the columns of R by α.

Lemma 3.1.B. If R is an $n^2 \times 3$ orthogonal array, then for every $\alpha \in S_3$ we have $R\alpha$ is also an orthogonal array.

Definition. If R is an orthogonal array, then it and the orthogonal array $R\alpha$ where $\alpha \in S_3$ (where S_3 is the symmetric group of three symbols) are *conjugate*. The associated quasigroups are also called *conjugate*.

Example 3.1.2. Consider the quasigroup $(Q, \circ)$ given below and $R\alpha$ where α is the permutation

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3),$$

where $(1, 2, 3)$ is the "cyclic notation" of the permutation:

1	1	1
1	2	3
1	3	4
1	4	2
2	1	4
2	2	2
2	3	1
2	4	3
3	1	2
3	2	4
3	3	3
3	4	1
4	1	3
4	2	1
4	3	2
4	4	4

R

1	1	1
3	1	2
4	1	3
2	1	4
4	2	1
2	2	2
1	2	3
3	2	4
2	3	1
4	3	2
3	3	3
1	3	4
3	4	1
1	4	2
2	4	3
4	4	4

$R(123)$

Definition. Two orthogonal arrays are *equal* if they define the same quasigroup.

Note 3.1.C. Equal orthogonal arrays will have the same rows, though the order of the rows of one array may be jumbled up in the second array. The orthogonal arrays R and $R(1,2,3)$ of Example 3.1.2 are equal (as can be tediously verified). Also, the quasigroup $(Q,\circ)$ defined by these orthogonal arrays (given in Example 3.1.1) satisfies the identity $(xy)x = y$ for all $x, y \in Q$. It is straightforward to verify this, but in fact any quasigroup invariant under conjugation by $\alpha = (1,2,3)$ (that is, any quasigroup equal to its conjugate under this permutation) satisfies this identity, as we now show. Let R be the orthogonal array associated with the quasigroup and let $x, y \in Q$. Then $(x, y, x \circ y) \in R$ (that is, it is a row of R), and applying the permutation we also have that $(x \circ y, x, y) \in R$. Therefore $(x \circ y) \circ x = y$ in $(Q,\circ)$, or $(xy)x = y$, as claimed. Notice that the converse also holds. That is, if $(Q,\circ)$ satisfies $(xy)x = y$ for all $x, y \in Q$ then the quasigroup is invariant under conjugation by $\alpha = (1,2,3)$ (which means that $R = R\alpha$). In Exercise 3.1.3, more identities are related to permutations in S_3.

Note. If a quasigroup $(Q,\circ)$ is invariant under conjugation by permutations α and β, then it (quite clearly) is invariant under conjugation by the permutation $\alpha\beta$. So the set of permutations in S_3 under which $(Q,\circ)$ is invariant under conjugations, is a set closed under the binary operation of permutation multiplication. This means that the set of these permutations forms a subgroup of S_3. See my online notes for Introduction to Modern Algebra (MATH 4127/5127) on Section I.5. Subgroups; notice Definition 5.4.

Definition. The subgroup of S_3 defined as

$$\{\alpha \mid (Q, \circ) \text{ is invariant under conjugation by } \alpha\}$$

is the *conjugate invariant subgroup* of $(Q, \circ)$.

Example 3.1.6. The quasigroup of Example 3.1.1,

$(Q, \circ) =$

$\circ$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

in invariant under conjugation by $\alpha = (1, 2, 3)$ as shown in Example 3.1.2. So it is also invariant under conjugation by $\alpha^2 = (1, 3, 2)$ and, of course, under conjugation by the identity permutation $\alpha^3 = (1)(2)(3)$. Now $(Q, \circ)$ is is not invariant under conjugation by $(1, 2)$, or else the identity $xy = yx$ would be satisfied by $(Q, \circ)$ (see Exercise 3.1.8). Similarly $(Q, \circ)$ is not invariant under conjugation by $(1, 3)$ or $(2, 3)$. Therefore, the conjugate invariant subgroup of $(Q, \circ)$ is $\langle(1, 2, 3)\rangle = \{(1)(2)(3), (1, 2, 3), (1, 3, 2)\}$ (that is, the subgroup of S_3 *generated* by element $(1, 2, 3) \in S_3$).

Definition. A quasigroup which has conjugate invariant subgroup of (all of) S_3 is *totally symmetric*. A quasigroup which is invariant under conjugation by (at least) $\langle(1, 2, 3)\rangle$ is *semisymmetric*.

Note 3.1.D. The quasigroup of Examples 3.1.1 and 3.1.6 is semisymmetric, but not totally symmetric. Notice from Exercise 3.1.8, a semisymmetric quasigroup satisfies the identity $x(yx) = y$ (or, equivalently, it satisfies the identity $(xy)x = y$). Also by Exercise 3.1.8, a symmetric quasigroup must satisfy these identities along with each of the identities $yx = yx$, $(yx)y = y$, and $x(xy) = y$. With a little group theory knowledge, we could show that if a quasigroup satisfies $x(yx) = y$ (or, equivalently, $(xy)x = y$) and any of the identities $yx = yx$, $(yx)y = y$, and $x(xy) = y$, then it is totally symmetric. We have seen that the subgroup generated by $(1, 2, 3)$ contains three permutations and we know that S_3 contains six permutations. By Lagrange's Theorem (see my Introduction to Modern Algebra [MATH 4127/5127] notes on Section II.10. Cosets and the Theorem of Lagrange; see Theorem 10.10) we have that the conjugate invariant subgroup of a quasigroup has 1, 2, 3, or 6 elements. If is contains $(1, 2, 3)$ then we know that it also contains the identity and $(1, 2, 3)^2 = (1, 3, 2)$ so that the conjugate invariant subgroup contains three permutations. It it contains any other permutation, then it must contain all six permutations of S_3.

Revised: 8/16/2022