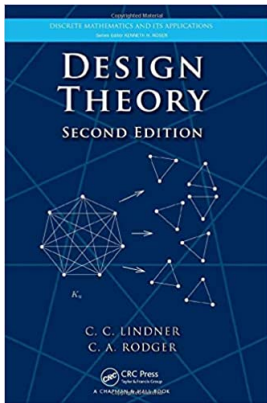


# Design Theory

## Chapter 3. Quasigroup Identities and Graph Decompositions

### 3.1. Quasigroup Identities—Proofs of Theorems



# Table of contents

1 Lemma 3.1.A

2 Lemma 3.1.B

# Lemma 3.1.A

**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.

**Proof.** Let  $a, b \in Q$ . We have  $a \circ b = c$  if and only if  $((a, b), c) := (a, b, c) \in R$ . For every pair of elements  $a, b \in Q$ , the equations  $a \circ x = b$  and  $y \circ a = b$  have unique solutions (namely,  $x$  and  $y$  where these are determined from the unique triple of type (2) of the form  $(a, x, b)$ ) and the unique triple of type (3) of the form  $(y, a, b)$  in  $R$  respectively). Therefore, by definition,  $(Q, \circ)$  is a quasigroup.  $\square$

# Lemma 3.1.A

**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.

**Proof.** Let  $a, b \in Q$ . We have  $a \circ b = c$  if and only if  $((a, b), c) := (a, b, c) \in R$ . For every pair of elements  $a, b \in Q$ , the equations  $a \circ x = b$  and  $y \circ a = b$  have unique solutions (namely,  $x$  and  $y$  where these are determined from the unique triple of type (2) of the form  $(a, x, b)$ ) and the unique triple of type (3) of the form  $(y, a, b)$  in  $R$  respectively). Therefore, by definition,  $(Q, \circ)$  is a quasigroup.  $\square$

## Lemma 3.1.B

**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.

**Proof.** Let  $(Q, \circ)$  be the quasigroup equivalent to orthogonal array  $R$ . Then  $a \circ b = c$  if and only if  $(a, b, c)$  is a row of  $R$  (by the definition of “orthogonal array”). We need to show that  $R\alpha$  is equivalent to some quasigroup. Notice that the entries of  $R$  and  $R\alpha$ , and the elements of  $Q$  are all the same.

## Lemma 3.1.B

**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.

**Proof.** Let  $(Q, \circ)$  be the quasigroup equivalent to orthogonal array  $R$ . Then  $a \circ b = c$  if and only if  $(a, b, c)$  is a row of  $R$  (by the definition of “orthogonal array”). We need to show that  $R\alpha$  is equivalent to some quasigroup. Notice that the entries of  $R$  and  $R\alpha$ , and the elements of  $Q$  are all the same.

Define binary operation  $\circ'$  on the elements  $Q$  as  $a \circ' b = c$  if and only if  $(a, b, c)$  is a row of  $R\alpha$  (since  $\alpha$  is a bijection on the rows of  $R$ , and the rows of  $R$  are not repeated, then the rows of  $R\alpha$  are not repeated). By the definition of quasigroup, we need to show that for every pair of entries in  $R\alpha$ ,  $a, b$ , the equations  $a \circ' x = b$  and  $y \circ' a = b$  have unique solutions. Now in  $(Q, \circ)$ , the equations  $a \circ x = b$  and  $y \circ a = b$  have unique solutions since  $(Q, \circ)$  is a quasigroup. So we relate the equations in  $\circ'$  to the equations in  $\circ$  using permutations in  $S_3$ .

## Lemma 3.1.B

**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.

**Proof.** Let  $(Q, \circ)$  be the quasigroup equivalent to orthogonal array  $R$ . Then  $a \circ b = c$  if and only if  $(a, b, c)$  is a row of  $R$  (by the definition of “orthogonal array”). We need to show that  $R\alpha$  is equivalent to some quasigroup. Notice that the entries of  $R$  and  $R\alpha$ , and the elements of  $Q$  are all the same.

Define binary operation  $\circ'$  on the elements  $Q$  as  $a \circ' b = c$  if and only if  $(a, b, c)$  is a row of  $R\alpha$  (since  $\alpha$  is a bijection on the rows of  $R$ , and the rows of  $R$  are not repeated, then the rows of  $R\alpha$  are not repeated). By the definition of quasigroup, we need to show that for every pair of entries in  $R\alpha$ ,  $a, b$ , the equations  $a \circ' x = b$  and  $y \circ' a = b$  have unique solutions. Now in  $(Q, \circ)$ , the equations  $a \circ x = b$  and  $y \circ a = b$  have unique solutions since  $(Q, \circ)$  is a quasigroup. So we relate the equations in  $\circ'$  to the equations in  $\circ$  using permutations in  $S_3$ .

## Lemma 3.1.B (continued 1)

**Proof (continued).** Consider what happens when we apply  $\alpha \in S_3$  to the position of the variables (first, second, or third position) in the equations  $a \circ' x = b$  and  $y \circ' a = b$ :

Permutation	Permuted Equations
(1)(2)(3)	$a \circ' x = b, y \circ' a = b$
(1, 2)	$x \circ' a = b, a \circ' y = b$
(1, 3)	$b \circ' x = a, b \circ' a = y$
(2, 3)	$a \circ' b = x, y \circ' b = a$
(1, 2, 3)	$b \circ' a = x, b \circ' y = a$
(1, 3, 2)	$x \circ' b = a, a \circ' b = y$

Taking the “variable” always as  $x$  and the “constants” as  $a$  and  $b$ , then each of the permuted equations is of one of the forms (we take constant  $a$  to the left of  $b$  in these forms):  $x \circ' a = b$ ,  $a \circ' x = b$ , or  $a \circ' b = x$ . Since  $\circ'$  is a binary operation, every equation of the form  $a \circ' b = x$  has a unique solution  $x$ .



## Lemma 3.1.B (continued 1)

**Proof (continued).** Consider what happens when we apply  $\alpha \in S_3$  to the position of the variables (first, second, or third position) in the equations  $a \circ' x = b$  and  $y \circ' a = b$ :

Permutation	Permuted Equations
(1)(2)(3)	$a \circ' x = b, y \circ' a = b$
(1, 2)	$x \circ' a = b, a \circ' y = b$
(1, 3)	$b \circ' x = a, b \circ' a = y$
(2, 3)	$a \circ' b = x, y \circ' b = a$
(1, 2, 3)	$b \circ' a = x, b \circ' y = a$
(1, 3, 2)	$x \circ' b = a, a \circ' b = y$

Taking the “variable” always as  $x$  and the “constants” as  $a$  and  $b$ , then each of the permuted equations is of one of the forms (we take constant  $a$  to the left of  $b$  in these forms):  $x \circ' a = b$ ,  $a \circ' x = b$ , or  $a \circ' b = x$ . Since  $\circ'$  is a binary operation, every equation of the form  $a \circ' b = x$  has a unique solution  $x$ .

## Lemma 3.1.B (continued 2)

**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.

**Proof (continued).** An equation of the form  $x \circ a = b$  has a unique solution in  $(Q, \circ)$ , so that  $(x, a, b)$  is a row of  $R$  exactly once. Since  $\alpha$  is a bijection of the rows of  $R$ , then  $(x, a, b)$  is a row of  $R\alpha$  exactly once. Therefore,  $x \circ' a = b$  has a unique solution. Similarly, an equation of the form  $a \circ x = b$  has a unique solution in  $(Q, \circ)$  so that  $(a, x, b)$  is a row of  $R$  exactly once,  $\alpha$  is a bijection of the rows of  $R$  and  $(x, a, b)$  is a row of  $R\alpha$  exactly once, therefore  $a \circ' ax = b$  has a unique solution. That is,  $(Q, \circ')$  is a quasigroup. Finally,  $R\alpha$  is the orthogonal array equivalent to this quasigroup, as claimed.  $\square$