Pacific Journal of Mathematics

SUB-QUASIGROUPS OF FINITE QUASIGROUPS

DRURY WILLIAM WALL

Vol. 7, No. 4 April 1957

SUB-QUASIGROUPS OF FINITE QUASIGROUPS

DRURY W. WALL

1. Introduction. Lagrange's theorem for finite groups (that the order of a sub-group divides the order of the group) does not hold for finite quasigroups in general. However, certain relationships can be obtained between the order of the quasigroup and the orders of its sub-quasigroups. This note will give some of these relationships.

DEFINITION. A set of elements Q and a binary operation "$\circ$" form a *quasigroup* $(Q, \circ)$ if and only if the following are satisfied:

I. If $a, b \in Q$ then there exists a unique $c \in Q$ such that $a \circ b = c$.

II. If $a, b \in Q$ then there exist $x, y \in Q$ such that $a \circ x = b$ and $y \circ a = b$.

III. If $a, x, y \in Q$ then either $a \circ x = a \circ y$ or $x \circ a = y \circ a$ implies $x = y$.

If $(Q, \circ)$ is a quasigroup and S is a subset of Q then $(S, \circ)$ is a sub-quasigroup of $(Q, \circ)$ if $(S, \circ)$ is a quasigroup.

Throughout this note the quasigroup operation will be written multiplicatively, that is, "ab" will be written for "$a \circ b$". Also, "Q" will be written to denote the quasigroup "$(Q, \circ)$". By quasigroup will be meant finite quasigroup, since only finite quasigroups will be considered. The order of a finite set X is the number of elements in X. For subsets X and Y of Q the symbols $X \cap Y$, $X \cup Y$ and $X \setminus Y$ will be used to denote the point set intersection, union and relative complement of X with Y, respectively.

The following elementary properties of a finite quasigroup Q will be of use.

P1. *If $X \subset Q$ and $a \in Q$ then X, aX and Xa have the same order.*

P2. *If $S \subset Q$ and S satisfies I then S is a sub-quasigroup of Q.*

Proof. To prove II, let $a, b \in S$. Since S satisfies I, $aS \subset S$ and by P1, $aS = S$. Thus, since $b \in S$ there exists an $x \in S$ such that $ax = b$. III is inherited from Q.

P3. *If S is a sub-quasigroup of Q then $a \in S$ and $b \notin S$ imply $ab \notin S$.*

2. Relationship of the order of any sub-quasigroup to the order of the quasigroup. The order of a sub-quasigroup need not divide the order of the quasigroup; in fact, these orders may be relatively prime. An example is given by Garrison [1, page 476] of a quasigroup of order 5 with a sub-quasigroup of order 2.

Received February 27, 1957, and in revised from June 15, 1957. Presented to the American Mathematical Society, August, 21, 1956.

THEOREM 1. *If Q is a quasigroup of order n and S is a sub-quasigroup of order S then $2s \leqq n$.*

Proof. Let $x \in Q \setminus S$. If $y \in S$ then $xy \in Q \setminus S$. Thus $xS \subset Q \setminus S$. But, by P1, xS has order s and since $Q \setminus S$ has order $n-s$ this implies that $s \leqq n-s$ or $2s \leqq n$.

This shows that the order of a sub-quasigroup is equal to or less than one half the order of the quasigroup. The quasigroup with two elements gives the simplest example in which the equality holds.

3. Relationship between the order of a quasigroup and the orders of two of its sub-quasigroups. Let Q be a quasigroup of order n and R and S be two proper sub-quasigroups of orders r and s, respectively. Assume that R and S intersect. Then $P=R \cap S$ is a sub-quasigroup of Q. Denote the order of P by p. Note that the subsets $R \setminus P$, $S \setminus P$, and $R \cup S$ are of orders $r-p$, $s-p$, and $r+s-p$, respectively.

THEOREM 2. $n \geqq r+s+\max(r, s)-2p$.

Proof. 1. Suppose $S \subset R$. Then $R \cap S=S$ and hence $p=s$, $s \leqq r$ and $\max(r, s)=r$. Thus,

$$r+s+\max(r, s)-2p=2r-s \leqq 2r .$$

But by Theorem 1, $2r \leqq n$ and so $r+s+\max(r, s)-2p \leqq n$.

2. Assume $R \setminus P$ and $S \setminus P$ are non-null. If $x \in R \setminus P$ and $y \in S \setminus P$ then $xy \notin R \cup S$. Thus, for $x \in R \setminus P$, $x(S \setminus P) \subset Q \setminus (R \cup S)$. But $x(S \setminus P)$ is of order $s-p$ and $Q \setminus (R \cup S)$ is of order $n-(r+s-p)$. Therefore, $s-p<n-(r+s-p)$. Similary, if $y \in S \setminus P$ then $y(R \setminus P) \subset Q \setminus (R \cup S)$ and thus, $r-p \leqq n-(r+s-p)$. Therefore,

$$n-(r+s-p) \geqq \max(r-p, s-p)=\max(r, s)-p$$

and so, $n \geqq r+s+\max(r, s)-2p$.

COROLLARY. *If $r=s$ then $n \geqq 3r-2p$.*

THEOREM 3. *If $n=r+s+\max(r, s)-2p$ then $r=s$ if and only if $T=P \cup [Q \setminus (R \cup S)]$ is a sub-quasigronp of Q.*

Proof. A. Assume $r=s$. Then R and S are sub-quasigroups of order r and T is a subset of order r. By P2, to show that T is a sub-quasigroup it suffices to show that if $x \in T$ and $y \in T$ then $xy \in T$.

(1) Let $x \in P$. Then if $y \in P$ then $xy \in P$ since P is a sub-quasigroup. If $y \in T \setminus P$ then $y \in Q \setminus (R \cup S)$ and hence $y \notin R$ and $y \notin S$. Hence $xy \notin R$, $xy \notin S$ and so $xy \in Q \setminus (R \cup S) = T \setminus P$. Thus if $x \in P$ and $y \in T$ then $xy \in T$.

(2) Let $x \in T \setminus P$ and $a \in R \setminus P$. First note that $xa \notin R$. For $b \in S \setminus P$, $ba \notin R \cup S$ and so $(S \setminus P)a \subset Q \setminus (R \cup S) = T \setminus P$. But $(S \setminus P)a$ and $T \setminus P$ are both of order $r-p$. Thus, $(S \setminus P)a = T \setminus P$ and since $x \notin S \setminus P$ this implies $xa \notin T \setminus P$ by III. Thus xa is in neither R nor $T \setminus P$ and so

$$xa \in Q \setminus [R \cup (T \setminus P)] = S \setminus P .$$

Thus, for $x \in T \setminus P$ it follows that $x(R \setminus P) \subset S \setminus P$. But $x(R \setminus P)$ and $S \setminus P$ are both of order $r-p$ and so $x(R \setminus P) = S \setminus P$. Similarly, it can be shown that $x(S \setminus P) = R \setminus P$. Thus, for

$$x \in T \setminus P, x[(R \setminus P) \cup (S \setminus P)] = [(R \setminus P) \cup (S \setminus P)] .$$

By noting that $T = Q \setminus [(R \setminus P) \cup (S \setminus P)]$ and by use of III, it follows that if $x \in T \setminus P$ and $z \in T$ then $xz \in T$. Combining parts (1.) and (2.), it follows that if $x \in T$ and $y \in T$ then $xy \in T$ and thus, T is a sub-quasigroup of Q.

B. Assume that T is a sub-quasigroup. T is of order $\max(r, s)$. Either $r > s$, $r < s$, or $r = s$. Assume $r > s$. Then $\max(r, s) = r$ and T and R are two sub-quasigroups of order r. Thus, by the Corollary to Theorem 2, $n \geqq 3r - 2p$. But, by hypothesis,

$$n = r + s + \max(r, s) - 2p = 2r + s - 2p .$$

Thus, $2r + s - 2p \geqq 3r - 2p$ and so $s \geqq r$, which is contrary to the assumption that $s < r$. Thus $r \not> s$. Similarly, $s \not> r$ and so $r = s$.

For the case in which R and S do not intersect the following results can be obtained.

THEOREM 2′. $n \geqq r + s + \max(r, s)$.

COROLLARY. *If* $r = s$ *then* $n \geqq 3s$.

THEOREM 3′. *If* $n = r + s + \max(r, s)$ *then* $r = s$ *if and only if* $Q \setminus (R \cup S)$ *is a sub-quasigroup of* Q.

An example of a group satisfying the hypothesis of Theorem 3 is the four group which has 3 subgroups of order 2 which intersect pairwise in the identity element. The following are examples of quasigroups satisfying the hypothesis of Theorem 3.

	a	b	c	d	e	f	g	h
a	a	b	c	d	f	e	g	h
b	b	a	d	c	e	f	h	g
c	c	d	a	b	g	h	f	e
d	d	c	b	a	h	g	e	f
e	f	e	h	g	b	a	d	c
f	e	f	g	h	a	b	c	d
g	h	g	e	f	c	d	a	b
h	g	h	f	e	d	c	b	a

Example 1.

	a	b	c	d	e	f
a	a	b	c	d	f	e
b	b	a	e	f	c	d
c	c	e	d	a	b	f
d	d	f	a	c	e	b
e	e	d	f	b	a	c
f	f	c	b	e	d	a

Example 2.

In Example 1, let $P=\{a, b\}$, $R=\{a, b, c, d\}$, $S=\{a, b, e, f\}$ and $T=\{a, b, g, h\}$. The hypothesis of Theorem 3 is satisfied and $r=s$ and T is a sub-quasigroup.

In Example 2, let $P=\{a\}$, $R=\{a, b\}$, $S=\{a, c, d\}$ and $T=\{a, e, f\}$. In this case $r\neq s$ and T is not a sub-quasigroup.

Counterexamples to many of the possible generalizations to more than two sub-quasigroups can be constructed. For example, it has been proved that (1) if Q is of order n with a subquasigroup of order s then $n\geqq 2s$ and (2) if Q is of order with two non-intersecting sub-quasigroups of order s then $n\geqq 3s$. Thus, it might be conjectured that for any positive integer m, if Q contains m mutually disjoint sub-quasigroups of order s then $n\geqq(m+1)s$. However, this fails for $m=3$ since it is possible to construct a quasigroup of order $3s$ with three disjoint sub-quasigroups of order s. In another direction, it is possible to construct a quasigroup of order $4s$ containing three disjoint sub-quasigroups of order s, in which the remaining s elements do not form a sub-quasigroup.

Reference

1. G. N. Garrison, *Quasi-groups*, Ann. of Math., **41** (1940), 474–487.

University of North Carolina

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. All other communications to the editors should be addressed to the managing editor, E. G. Straus at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics

Vol. 7, No. 4 April, 1957