HOMOGENEOUS QUASIGROUPS

SHERMAN K. STEIN

A mathematical system whose group of automorphisms is transitive we will call homogeneous. If the group of automorphisms is doubly transitive, then we will call the system doubly homogeneous. We examine here homogeneous and doubly homogeneous finite quasigroups.

We prove that there are no homogeneous quasigroups whose order is twice an odd number (Theorem 1.1). As the quasigroups satisfying the identity $X(YZ) = XY \cdot XZ$ show, there are homogeneous quasigroups of all other orders ([5], p. 236).

We then examine doubly homogeneous quasigroups and show that they are intimately connected with nearfields (Theorem 2.2). Since all finite nearfields are known, we thus have a complete description of the doubly homogeneous quasigroups.

In the last two sections we obtain various equivalent descriptions of double homogeneity and apply them to the construction of block designs and models for certain identities.

1. Homogeneous quasigroups. In this section two theorems are obtained that generalize results concerning distributive quasigroups.

THEOREM 1.1. *There is no homogeneous quasigroup of order* $4k + 2$.

Proof. Let $(Q, \circ)$ be a homogeneous quasigroup of order $4k + 2$. We first construct out of this quasigroup an idempotent homogeneous quasigroup of order $4k + 2$.

Define $f: Q \to Q$ by $f(x) = x \circ x$. We assert that f is onto Q, and hence a bijection. Indeed, let a be a fixed element of Q, $b = a \circ a$, c an arbitrary element of Q, g an automorphism of $(Q, \circ)$ such that $g(b) = c$. We then have

$$c = g(b) = g(a \circ a) = g(a) \circ g(a) = f(g(a)) .$$

Thus f is onto Q.

We thus can define a quasigroup $(Q, \odot)$, isotopic to $(Q, \circ)$, by $f(x) \odot f(y) = x \circ y$. Since $f(x) \odot f(x) = x \circ x = f(x)$, $(Q, \odot)$ is idempotent. Moreover, if g is an automorphism of $(Q, \circ)$, it is also an automorphism of $(Q, \odot)$, since

Received January 11, 1963, and in revised form September 5, 1963.
This work was partly sponsored by the Air Force Office of Scientific Research.

$$g(f(x)) \odot f(y)) = g(x \circ y) = g(x) \circ g(y)$$

and

$$g(f(x) \odot g(f(y)) = (g(x \circ x)) \odot (g(y \circ y)) = (g(x) \circ g(x)) \odot (g(y) \circ g(y))$$
$$= f(g(x)) \odot f(g(y)) = g(x) \circ g(y) .$$

Thus $(Q, \odot)$ is an idempotent homogeneous quasigroup of order $4k + 2$. By ([5], p. 237), such quasigroups do not exist, and the theorem is proved.

As was shown in [6], if Q is a left-distributive quasigroup, then there is a quasigroup A' orthogonal to it. The next theorem generralizes this fact. The proof makes use of the notion of transversal for a quasigroup, $(Q, \circ)$, of order n. A transversal for $(Q, \circ)$ is a set $T \subset Q \times Q$, $T = \{(x_1, y_1), \cdots, (x_n, y_n)\}$ such that $x_i = x_{i'}$ implies $i = i'$, $y_j = y_{j'}$ implies $j = j'$, and $x_i \circ y_i = x_j \circ y_j$ implies $i = j$. It is easily seen that there is a quasigroup orthogonal to $(Q, \circ)$ if and only if there are n disjoint transversals for Q.

THEOREM 1.2. *If $(Q, \circ)$ is a quasigroup of order n possessing a transitive set of n automorphisms, then there is a quasigroup orthogonal to it.*

Proof. Let $\phi_1, \phi_2, \cdots, \phi_n$ be a transitive set of n automorphisms of $(Q, \circ)$ and $Q = \{b_1, b_2, \cdots, b_n\}$. We shall define n disjoint transversals for Q, $T(1), T(2), \cdots, T(n)$, where $T(k) \subset Q \times Q$, $k = 1, 2, \cdots, n$. Select $a \in Q$ and let

$$T(k) = \{(\phi_i(a), \phi_i(b_k)) \mid 1 \leqq i \leqq n\} .$$

The first coordinates of the n elements of $T(k)$ are distinct and so are the second coordinates; also $T(i) \cap T(j) = \phi$ if $i \neq j$.

It must be shown that $\phi_i(a) \circ \phi_i(b_k) = \phi_j(a) \circ \phi_j(b_k)$ implies that $i = j$. From the assumed equation it follows that $\phi_i(a \circ b_k) = \phi_j(a \circ b_k)$. Since the n automorphisms $\phi_1, \cdots, \phi_n$ are transitive on a set of n elements, it follows that if ϕ_i and ϕ_j agree on a single element of Q then $\phi_i = \phi_j$; thus $\phi_i = \phi_j$, and the theorem is proved.

2. Relations between doubly homogeneous quasigroups and nearfields. Consider a finite doubly homogeneous groupoid $(G, \circ)$. For any order n the two groupoids defined by $x \circ y = x$ or $x \circ y = y$ are doubly homogeneous (in fact any bijection of G is an automorphism of $(G, \circ)$). Also the groupoid of order 2 given by $1 \circ 1 = 2$, $2 \circ 2 = 1$, $1 \circ 2 = 2$, $2 \circ 1 = 1$, and its transpose are doubly homogeneous. We will show that the only other doubly homogeneous groupoids are quasigroups

THEOREM 2.1. *A doubly homogeneous groupoid* $(G, \circ)$ *is either*:
(i) *The groupoid defined by* $x \circ y = x$, *for all* $x, y \in G$,
(ii) *The groupoid defined by* $x \circ y = y$ *for all* $x, y \in G$,
(iii) *An idempotent doubly homogeneous quasigroup, or*
(iv) *A groupoid isomorphic to the groupoid defined above.*

Proof. First let us show that if the order of G is at least 3, then $(G, \circ)$ is idempotent. To do so, let $c, d \in G$, $c \neq d$, $c \circ c = d$. Let $e \in G$, $e \neq c, d$, and ϕ be an automorphism of $(G, \circ)$ such that

$$\phi(c) = c, \phi(d) = e .$$

Then we have

$$c \circ c = d \text{ and } c \circ c = \phi(c) \circ \phi(c) = \phi(c \circ c) = \phi(d) = e ,$$

a contradiction that implies $c \circ c = c$.

Assume that $a, b \in G$, $a \neq b$. If $a \circ b = a$, then the double homogeneity of $(G, \circ)$ implies that $x \circ y = x$ for all $x, y \in G$. Similarly, if $a \circ b = b$, then $x \circ y = y$ for all $x, y \in G$.

Consider finally the case, $a \circ b = c$, $c \neq a, b$. Double homogeneity implies that the equations $A \circ Y = C$ and $X \circ B = C$ have solutions, X, Y if $A \neq C$, $B \neq C$. Combining this with the idempotency of $(G, \circ)$, we see that if $(G, \circ)$ has order at least 3, then it is a quasigroup.

The case of order 2 is left to the reader.

In view of Theorem 2.1, we will examine doubly homogeneous quasigroups.

In the rest of this paper we will generally assume that all quasigroups are idempotent. An idempotent quasigroup that can be generated by two elements will be called a two-generated quasigroup. A two-quasigroup is a doubly homogeneous two-generated quasigroup. We will show that two-quasigroups and finite nearfields are closely related.

A finite near field, S, consists of a finite set S and two binary operations, $+$ and $.$, defined on all of S. The operation $+$ is an abelian group, the operation $.$, restricted to $S - \{0\}$ is a group, and left distributivity holds, $a(b + c) = ab + ac$. From these conditions it follows that $a0 = 0 = 0a$ and $(-1)a = -a = a(-1)$ (see [8, pp. 188–190]), and that the equation $ax + bx = c$ has a unique solution if $a + b \neq 0$. Moreover, it is implicit in [8] that a finite nearfield has a primitive element.

THEOREM 2.2. *If* $(S, \circ)$ *is a two-quasigroup, then there is a nearfield* $(S, +, .)$ *and primitive element* k *such that* $x \circ y = x + (y - x)k$.

The automorphisms of $(S, \circ)$ *are of the form* $\phi(x) = a + bx$.

Proof. The group G of automorphisms of $(S, \circ)$ is doubly transitive and only the identity automorphism fixes two elements of S. Such a group of permutations on a finite set determines a near field as follows ([9], p. 25, [2], pp. 385–388).

The elements of G leaving no elements fixed, together with the identity transformation, form an abelian, simply transitive normal subgroup N of G. Select an element $0 \in S$. We define $x + y$ as follows. There is a unique $\sigma \in N$, such that $\sigma(0) = x$; define $x + y$ to be $\sigma(y)$.

We define $x \cdot y$ as follows. Select $1 \in S$, $1 \neq 0$. Define $x \cdot y$ to be $\tau(y)$ where $\tau(0) = 0$, $\tau(1) = x$. Then $(S, +, .)$ is a nearfield. Moreover, since $\sigma(x) = x + b$ and $\tau(x) = ax$ $(a \neq 0)$ are automorphisms of $(S, \circ)$, then so is $\phi(x) = ax + b$. Since there are (n) $(n - 1)$ such ϕ's, where n is the cardinality of S, it follows that every automorphism of $(S, \circ)$ has the form $\phi(x) = ax + b$.

Next, we express the quasigroup $(S, \circ)$ in terms of the nearfield $(S, +, .)$ just constructed. Let $0 \circ 1 = k$. If $x, y \in S$, $x \neq y$, let ϕ be the automorphism of $(S, 0)$ such thar $\phi(0) = x$, $\phi(1) = y$, that is, $\phi(u) = x + (y - x)u$ for all $u \in S$. Then we have

$$x \circ y = \phi(0) \circ \phi(1) = \phi(0 \circ 1) = \phi(k) = x + (y - x)k, \quad (x \neq y).$$

Since $x \circ x = x + (x - x)k$, $(S, \circ)$ is of the asserted form.

COROLLARY 2.3. *A commutative two-quasigroup* $(Q, \circ)$ *is of (odd) prime order,* p, *and is expressible in terms of* $GF(p)$, *the Galois field of* p *elements, by the formula* $x \circ y = (x + y)/2$.

Proof. $(Q, \circ)$ is expressible in terms of a nearfield $(Q, +, .)$ by the formula $x \circ y = x + (y - x)k$. Since $(Q, \circ)$ is commutative, $0 \circ 1 = 1 \circ 0$. Thus

$$k = 0 \circ 1 = 1 \circ 0 = 1 - k,$$

hence

$$k + k = 1.$$

By left distributivity $k \cdot 2 = 1$. Now, the element 1 in any finite nearfield generates a Galois field with a prime number of elements, say p elements. The equation $k \cdot 2 = 1$ shows that $p \neq 2$ and that k is an element of that Galois field. Since k is a primitive element of $(Q, +, .)$, we see that $(Q, +, .)$ is the Galois field with p elements, and $x \circ y = x + (y - x)(1/2) = (x + y)/2$.

The next corollary relates doubly homogeneity to the identity

$(x \circ y) \circ (z \circ w) = (x \circ z) \circ (y \circ w)$, which has several names, including "the medial law".

COROLLARY 2.4. *A two-generated quasigroup* $(S, \circ)$ *of prime order* p, *is medial if and only if it is doubly homogeneous.*

Proof. If $(S, \circ)$ is doubly homogeneous, then it is of the form $x + (y - x)k$, for some nearfield. But the only near fields of prime order are the Galois fields. Thus $x \circ y = (1 - k)x + ky$ and a simple computation shows that satisfies the identity $(x \circ y) \circ (z \circ w) = (x \circ z) \circ (y \circ w)$ Hence $(S, \circ)$ is medial.

Conversely, if $(S, \circ)$ is medial, it is of the form $x \circ y = A(x) + B(y)$ where $(S, +)$ is an abelian group on p elements, and A and B are automorphisms of $(S, +)$ such that $A(x) + B(x) = x$, for all $x \in S$ (see [4]). But $(S, +)$ can be imbedded in the larger structure $(S, +, .)$, the Galois field of p elements, in such a way that every automorphism, ϕ, of $(S, +)$ is of the form $\phi x = ax$ for some $a \in S$. Thus $A(x) = (1 - k)x$ and $B(x) = kx$ for some k. Hence we have $x \circ y = x + (y - x)k$ and so $(S, \circ)$ is doubly homogeneous.

THEOREM 2.5. *Let* $(S, +, .)$ *be a finite nearfield and* $k \in S$, $k \neq 0, 1$. *Define a binary operation* $\circ$ *on* S *by* $x \circ y = x + (y - x)k$. *Then* $(S, \circ)$ *is a doubly homogeneous quasigroup.* $(S, \circ)$ *is a two-quasigroup if and only if* k *is a primitive element of* S.

Proof. It is easy to see that $(S, \circ)$ is a quasigroup. For example, if $x \circ y = x' \circ y$, then

$$x + (y - x)k = x' + (y - x')k$$

and so

$$(x - x') = (x - y)k + (y - x')k .$$

But we also have

$$(x - x') = (x - y)1 + (y - x')1 .$$

By the definition of a nearfield and the fact that $k \neq 1$, we obtain $x = x'$.

For $a, b \in S$, $a \neq 0$, define $\phi: S \to S$ by $\phi(x) = ax + b$. Each ϕ is an automorphism of $(S, \circ)$ and the collection of all such ϕ's is doubly transitive on S. Thus $(S, \circ)$ is a doubly homogeneous quasigroup.

If $(S, \circ)$ is a two-quasigroup, it is generated, as a quasigroup, by any two of its elements, in particularly by $\{0, 1\}$. Now, the nearfield in $(S, +, .)$ generated by k contains 0 and 1; thus k is a primitive

element of $(S, +, .)$ Finally, we must show that if k is a primitive element of $(S, +, .)$, then $\{0, 1\}$ generates the quasigroup $(S, \circ)$. To do so, let $(T, \circ)$ be the subquasigroup of $(S, \circ)$ generated by $\{0, 1\}$. We will show that $T = S$.

First of all, $(T, \circ)$ is doubly homogeneous. Indeed, if $a, b \in T$, $a \neq b$, and ϕ is an automorphism of $(S, \circ)$ such that $\phi(0) = a$, $\phi(1) = b$, then $\phi(T)$ is contained in the quasigroup generated by $\{a, b\}$. Since T and $\phi(T)$ have the same cardinality, $\phi(T) = T$, and $\phi \mid T$ is an automorphism of $(T, \circ)$, taking 0 into a, and 1 into b.

Thus, by Theorem 2.2, $(T, \circ)$ is related to a nearfield $(T, \oplus, \odot)$ by the formula $x \circ y = x \oplus (y \ominus x) \odot k'$, where $(T, \oplus, \odot)$ can be chosen to have the same 0 and 1 as $(S, +, .)$ [$\ominus$ denotes subtraction in $(T, \oplus, \odot)$]. We will show that $\oplus$ and $\odot$ are restrictions of $+$ and $.$, and thus $(T, \oplus \odot)$ is a subnearfield of $(S, +, .)$.

Note first that since $0 \oplus (1 \ominus 0) \odot k' = 0 \circ 1 = 0 + (1 - 0)k$, we have $k = k'$ and thus $k \in T$. Next we will show that $x \oplus y = x + y$ and $x \odot y = x \cdot y$ for all $x, y \in T$.

For $x = 0$, it is obvious that $x \oplus y = x + y$. Let $x \in T$, $x \neq 0$, and $\phi : S \to S$ be the automorphism of $(S, \circ)$ given by $\phi(y) = x + y$. Then $\phi \mid T$ is an automorphism of $(T, \circ)$ without fixed points. Thus $(\phi \mid T)y = u \oplus y$ for some fixed $u \in T$ and all $y \in T$. Since $u = (\phi \mid T)(0) = \phi(0) = x$, we have $u = x$. Thus $x \oplus y = (\phi \mid T)y = \phi(y) = x + y$ for all $x, y \in T$.

To show $x \odot y = x \cdot y$ for all $x, y \in T$, we proceed similarly. For $x = 0$ or 1 the statement is trivial. Let $x \neq 0, 1$, $x \in T$. Let $\phi : S \to S$ be defined by $\phi(y) = x \cdot y$. Then $\phi \mid T$ is an automorphism of $(T, \circ)$ with the one fixed element, 0. Thus $(\phi \mid T)(y) = u \odot y$ for some u. Since $u = u \odot 1 = (\phi \mid T)(1) = \phi(1) = x \cdot 1 = x$, we have $u = x$. Hence $x \odot y = (\phi \mid T)y = \phi(y) = x \cdot y$, for all $x, y \in T$.

Thus $(T, \oplus, \odot)$ is a subnearfield of $(S, +, .)$ and contains the element k. Since k is a primitive element of the nearfield S, we must have $S = T$. Thus $(S, \circ)$ is generated by $\{0, 1\}$ and therefore is a two-quasigroup.

COROLLARY 2.6. *If k is a primitive element of a nearfield S, then $\{0, k\}$ generates S by the single binary operation $x \circ y = x + (y - x)k$.*

The relation between quasigroups and near fields is shown further in the following theorems. For simplicity if k is an element of a nearfield $(Q, +, .)$, then the quasigroup $(Q, \circ)$ defined by $x \circ y = x + (y - x)k$ we denote $Q(k)$.

THEOREM 2.7. *If $(Q, +, .)$ is a nearfield, $k, k' \in Q$ and $\phi : Q \to Q$*

is an automorphism of $(Q, +, .)$ *such that* $\phi(k) = k'$, *then* ϕ *is an isomorphism between* $Q(k)$ *and* $Q(k')$.

Proof. Let $\circ$ denote multiplication in $Q(k)$ and $\odot$ denote multiplication in $Q(k')$. Then $\phi(x \circ y) = \phi(x + (y - x)k) = \phi(x) + (\phi(y) - \phi(x))k' = \phi(x) \odot \phi(y)$. Thus ϕ is an isomorphism of $Q(k)$ onto $Q(k')$.

The next theorem is the converse of Theorem 2.7.

THEOREM 2.8. *If* $(Q, +, .)$ *is a nearfield,* k, k' *are primitive elements of* $(Q, +, .)$, *and* $Q(k)$ *is isomorphic to* $Q(k')$, *then there is an automorphism* ϕ *of* $(Q, +, .)$ *such that* $\phi(k) = k'$.

Proof. Let $\alpha: Q(k) \to Q(k')$ be an isomorphism between the quasigroups $Q(k)$ and $Q(k')$. Let $\circ$ and $\odot$ be the operations in $Q(k)$, $Q(k')$ respectively. Since $Q(k)$ is doubly homogeneous, we may assume that $\alpha(0) = 0$ and $\alpha(1) = 1$. Then

$$\alpha(k) = \alpha(0 \cdot 1) = \alpha(0) \odot \alpha(1) = 0 \odot 1 = k'$$

We will show that α is an automorphism of $(Q, +, .)$.

Let σ be an antomorphism of $Q(k)$ defined by $\sigma(x) = x + b$, $b \neq 0$. Then, $\alpha\sigma\alpha^{-1}$, being an automorphism of $Q(k')$ and having no fixed elements, is of the form $x \to x + c$ for some fixed c. Thus $\alpha\sigma(t) = \alpha(t) + c$ for all $t \in Q$; equivalently, $\alpha(t + b) = \alpha(t) + c$. In particular, $\alpha(b) = \alpha(0 + b) = \alpha(0) + c = c$, and we have $\alpha(t + b) = \alpha(t) + \alpha(b)$. That is, α is an automorphism of $(Q, +)$.

Similarly, let $\sigma: Q(k) \to Q(k)$ be given by $\sigma(x) = ax$. Since σ is an automorphism of $Q(k)$ with $\sigma(0) = 0$, $\alpha\sigma\alpha^{-1}$ is an automorphism τ of $Q(k')$ with $\tau(0) = 0$. Thus $\tau(x) = a'x$ for some $a' \in Q$. We have $\alpha\sigma(x) = \tau\alpha(x)$, or equivalently, $\alpha(ax) = a'\alpha(x)$. But $\alpha(1) = 1$; hence $\alpha(a) = \alpha(a \cdot 1) = a'\alpha(1) = a' \cdot 1 = a'$. Thus $\alpha(ax) = \alpha(a)\alpha(x)$, and α is an automorphism of $(Q, \cdot)$. This ends the proof.

As another application of Theorem 2.2 we have

THEOREM 2.9. *A left-distributive two-quasigroup is medial (hence right-distributive).*

Proof. Let $(Q, \circ)$ be a left-distributive two-quasigroup. By Theorem 2.2, $x \circ y = x + (y - x)k$ for some nearfield $(Q, +, .)$. Since left translation by 0 is an automorphism of $(Q, \circ)$, there exist $a, b \in Q$ such that

$$0 \circ x = a + bx \qquad \text{for all } x \in Q.$$

Thus $xk = a + bx$ for all $x \in Q$.

It is easy to see that $a = 0$ and $b = k$, by letting $x = 0, 1$. Thus $xk = kx$ for all $x \in Q$. Since k is a primitive element of $(Q, +, .)$, the nearfield in question is commutative, hence a field. The theorem follows immediately.

It might be remarked that a quasigroup and its conjugates [5] have the same automorphisms. Thus the conjugate of a two-quasigroup is a two-quasigroup. If $x \circ y = z$ then two of the six conjugate operations, α and β, are defined by $x\alpha z = y$ and $y\beta z = x$. Here α and β denote division on the left and right respectively. It turns out that α and β are easily expressed in terms of the nearfield describing $\circ$. For if $x \circ y = x + (y - x)k = z$, then $y = x + (z - x)k^{-1}$. Also, it can be shown that if $x \circ y = z$ then $x = y + (z - y)(1 - k)^{-1}$.

3. **Two-homogeneity and identities.** Let Q be a finite idempotent quasigroup and $\Phi(Q)$ be the identities valid on Q [7]. Let F be the free groupoid on two generators x, y and $F(Q)$ be the homomorphic image of F obtained from F through factoring F by $\Phi(Q)$. That is, define an equivalence relation, $\sim$, on F as follows: If $U, V \in F$ and $U = V$ is an identity valid on Q, write $U \sim V$. Then $F(Q)$ is $F/\sim$. It is easily seen that $F(Q)$ is a finite idempotent quasigroup. Note also that if $U \in F$ and $a, b \in Q$, then replacement of x and y in U by a and b defines an element in Q; we denote this element, $U(a, b)$. We may denote U itself as $U(x, y)$. If $U \in F$, then U determines a unique element of $F(Q)$, denoted $\tilde{U}$.

THEOREM 3.1. *Let Q be a quasigroup generated by $\{a, b\}$, and assume that for all $U, V \in F$ such that $U(a, b) = V(a, b)$, one also has the identity $U(x, y) = V(x, y)$ valid on Q. Then Q is isomorphic to $F(Q)$. The converse holds.*

Proof. Since Q satisfies all the identities that $F(Q)$ satisfies, there is a homomorphism $h: F(Q) \to Q$ such that $h(\tilde{x}) = a$, $h(\tilde{y}) = b$. Also we can define a function $k: Q \to F(Q)$ by setting $k(a) = \tilde{x}$ and $k(b) = \tilde{y}$, and extending this assignment to a homomorphism. (The possibility of defining this k is equivalent to the hypothesis made on a and b.) Clearly h and k are inverse to each other, hence isomorphisms.

Conversely, assume that $h: F(Q) \to Q$ is an isomorphism. Let $a = h(\tilde{x})$, $b = h(\tilde{y})$. If $U(a, b) = V(a, b)$, then $h[\widetilde{U(x, y)}] = h[\widetilde{V(x, y)}]$. Since h is an injection, $\widetilde{U(x, y)} = \widetilde{V(x, y)}$. Thus $U \sim V$, which was to be proved.

COROLLARY 3.2. A two-quasigroup Q is isomorphic to $F(Q)$.

It should be noted that for a quasigroup Q, $F(Q)$ is doubly homogeneous if and only if it is generated by any pair of elements. And when $F(Q)$ is a two-quasigroup, any two elements of Q generate a quasigroup isomophic to $F(Q)$.

COROLLARY 3.3. *Two two-quasigroups are isomorphic if and only if they have the same identities in two variables.*

COROLLARY 3.4. *A two-generated quasigroup Q is doubly homogeneous if and only if for all distinct $a, b \in Q$ and all distinct $c, d \in Q$, $U(a, b) = V(a, b)$ is equivalent to $U(c, d) = V(c, d)$ for all terms U, V in two variables.*

Proof. Clearly, if $\{a, b\}$ generates Q, so does $\{c, d\}$. Then apply Theorem 3.1 and the remarks preceding Corollary 3.3.

As already mentioned, a two-quasigroup is defined by its identities in two variables. In fact, if Q is a two-quasigroup of order n, then Q can be defined by $n^2 - n + 1$ identities, namely the identity $X^2 = X$ and an identity corresponding to each product $u_i(a, b) \cdot u_j(a, b) = u_k(a, b)$, $i \neq j$, where each element of Q is represented in the form $u_s(a, b)$ for some term in a and b. Let us consider, for example, the only two-quasigroup of order four, Q, given by:

	a	b	ab	ba
a	a	ab	ba	b
b	ba	b	a	ab
ab	b	ba	ab	a
ba	ab	a	b	ba

Since $a \cdot ab = ba$ and $ab \cdot ba = a$, Q satisfies the identities:

(i) $X \cdot XY = YX$ and

(ii) $XY \cdot YX = X$. We will show that (i) and (ii) are sufficient to reconstruct the multiplication table for Q. This will be useful in § 4.

THEOREM 3.5. *A finite groupoid Q' satisfying the identities* (i), $X \cdot XY = XY$ *and* (ii), $XY \cdot YX = X$ *is a quasigroup. Moreover any two distinct element $a, b \in Q'$ generate a quasigroup Q'' described by the preceding multiplication table.*

Proof. Let L and R be a left-and right translation in Q' by the same element. By (i), $LL = R$. We prove that L is an injection.

Let $c, d, e \in Q'$ and $cd = ce$. We will show that $d = e$. We have $c \cdot cd = c \cdot ce$ and, by (i), $dc = ec$. Thus $dc \cdot cd = ec \cdot ce$. By (ii),

$d = e$. Thus Q' is a quasigroup.

Since Q' satisfies $X \cdot XY = YX$, it satisfies $X \cdot XX = XX$. Since Q' is a quasigroup it must therefore satisfy $XX = X$; thus Q' is idempotent.

We next show that distinct elements of Q' do not commute. Assume that $c, d \in Q'$, $cd = dc$. Then, by (ii) we have $c = cd \cdot dc = dc \cdot cd = d$.

Now let us examine the quasigroup Q'' generated by a and b. First of all, Q'' is an idempotent quasigroup and $ab \neq ba$. Thus Q'' has at least the four distinct elements a, b, ab, ba. We will show that Q'' has no more elements.

From (i) and (ii) we obtain $XY(XY \cdot YX) = XY \cdot X$, hence $YX \cdot XY = XY \cdot X$ and thus $Y = XY \cdot X$. From $Y = XY \cdot X$ follows $Y = X \cdot YX$ [7]. Also, $XY \cdot Y = XY(XY \cdot X) = X \cdot XY = YX$.

From these identities follow: $aa = a$, $bb = b$, $ab \cdot ab = ab$, $ba \cdot ba = ba$; $a \cdot ab = ba$, $a \cdot ba = b$, $b \cdot ab = a$, $b \cdot ba = ab$; $ab \cdot a = b$, $ab \cdot b = ba$, $ab \cdot ba = a$; $ba \cdot a = ab$, $ba \cdot b = a$, $ba \cdot ab = b$. Thus Q' has only the four elements a, b, ab, ba. Moreover its multiplication table is the one already given.

4. **Block designs and quasigroups.** By a pairwse balanced incomplete block design on a set S we will mean a family of subsets $B_1, B_2, \cdots, B_r$ of S, each containing the same number of elements, $k \geq 3$, such that each pair of elements of S is a subset of exactly one of the B's. If $(S, \circ)$ is a doubly homogeneous quasigroup, then the two-generated subquasigroups of S form a pairwise balanced incomplete block design (for brevity, block design). Calling the cardinality of S, v, we then have a doubly transitive block design $B(k, v)$ where k, incidentally, is a power of a prime. The following theorems show various relations between block designs and algebraic aspects of quasigroups.

THEOREM 4.1. *A two-generated quasigroup Q is doubly homogeneous (hence a two-quasigroup) if and only if the two-generated subquasigroups of $Q \times Q$ all have the same order.*

Proof. Assume that Q is a two-quasigroup of cardinality q. Consider the quasigroup $Q^* \subset Q \times Q$ generated by $\{(a, c), (b, d)\}$, where a, b, c, and d are distinct. Let $\pi : Q \times Q \to Q$ be the projection defined by $\pi(q_1, q_2) = q_1$. Then $\pi(Q^*) = Q$ since Q is generated by any two of its elements, in particular, a and b. Now, for any U and V, terms in the variables x and y, $U((a, c), (b, d)) = V((a, c), (b, d))$ if and only if, $U(a, b) = V(a, b)$ and $U(c, d) = V(c, d)$. By Corollary 3.4, $U(a, b)$

$= V(a, b)$ if and only if $U(c, d) = V(c, d)$. Thus π is an isomorphism onto Q, and $\{(a, c), (b, d)\}$ generates a quasigroup of order q. Special cases such as $\{(a, b), (b, b)\}$, $\{(a, b), (a, b)\}$ or $\{(a, b), (c, a)\}$ are easily disposed of.

Conversely, assume that Q^*, of order q, is two-generated and that every two elements of $Q \times Q$ generate a quasigroup of the same order, necessarily q. We will show that Q is doubly homogeneous. Let $\{a_1, a_2\}$ and $\{b_1, b_2\}$ be two distinct pairs of elements of Q, $a_1 \neq a_2$, $b_1 \neq b_2$. Then $a = (a_1, a_2)$ and $c = (b_1, a_2)$ generate a quasigroup of order q; thus a and $b = (b_1, b_2)$ generate a quasigroup Q^* such that $\pi(Q^*) = Q$. This implies that two elements of Q^* are equal if their first coordinates are equal. Thus $U(a_1, b_1) = V(a_1, b_1)$ is equivalent to $U(a_2, b_2) = V(a_2, b_2)$. By Corollary 3.4, Q is a two-quasigroup.

The notion of two-quasigroup can be used to give a simple proof of the following combinatorial theorem due to Skolem [1, p. 183].

THEOREM 4.2 *If k is a prime power and $B(k, v_1)$ and $B(k, v_2)$ exist, then $B(k, v_1v_2)$ exists.*

Proof. Let $B(k, v_i)$ be a block design on the set S_i, $i = 1, 2$. Select a two-quasigroup Q of order k. On each block of $B(k, v_1)$ and $B(k, v_2)$ define a quasigroup isomorphic to Q. This defines on S_i a quasigroup Q_i, $i = 1, 2$, such that every two elements of S_i generate a quasigroup isomorphic to Q. Every two elements of $Q_1 \times Q_2$ generate a quasigroup R satisfying all the identities that Q satisfies. Since $Q = F(Q)$, R is a homomorphic image of Q. As a two-quasigroup contains no proper subquasigroups, (other than those with one element), R is isomorphic to Q. This shows that on $S_1 \times S_2$ there is a $B(k, v_1v_2)$.

THEOREM 4.3. *There is a quasigroup of order v satisfying the identities $X \cdot XY = YX$ and $XY \cdot YX = X$ if and only if $v = 12n + 1$ or $v = 12n + 4$.*

Proof. Recalling the example at the end of §3 and the argument in the proof of Theorem 4.2, we see that such quasigroups exist if and only if there is a $B(4, v)$. As Hanani proved in [3], a $B(4, v)$ exists if and only if $v = 12n + 1$ or $v = 12n + 4$.

Similar reasoning shows that if an identity in two letters has a two-quasigroup model of order k, and there is a $B(k, v)$, then the identity has a model of order v. In particular, since $X \cdot XY = YX$ has a two-quasigroup model of order 5, it has, by [3], models of all orders of the form $20n + 1$ or $20n + 5$ (except possibly 141).

REFERENCES

1. R. C. Bose and S. S. S. Shrikhande, *On the composition of incomplete block designs*, Canadian Math. J., **12** (1960) 177-188.
2. M. Hall, *The theory of groups*, Macmillan, NY, 1959.
3. H. Hanani, *The existence and construction of balanced incomplete block designs*, Ann. Math. Stat., **32** (1961), 361-386.
4. D. C. Murdoch, *Structure of abelian quasigroups*, Trans. Amer. Math. Soc., **49** (1951), 392-409.
5. S. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc., **85** (1957), 228-256.
6. ———, *Left-distributive quasigroups*, Proc. Amer. Math. Soc., **10** (1959), 557-558.
7. ———, *Finite models of identities*, ibid, **14** (1963), 216-222.
8. H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Hamburg, **11** (1935), 187-220.
9. ———, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, ibid, pp. 17-40.

UNIVERSITY OF CALIFORNIA AT DAVIS