VARIETIES OF P-QUASIGROUPS

Darryn E. Bryant[1]
Centre for Combinatorics
Department of Mathematics
The University of Queensland
Queensland 4072
Australia

ABSTRACT

Decompositions of complete undirected graphs into sets of closed trails which partition the edge set of the graph and which contain each pair of distinct vertices exactly once at distance 2 define and are defined by a class of quasigroups called P-quasigroups. Conditions are established under which P-quasigroups are (or are not) homomorphic images of P-quasigroups which possess certain properties. The variety generated by the class of quasigroups arising from all 2-perfect m-cycle systems (uniform m-P-quasigroups) is thereby determined for all positive integers m, ($m \neq 1, 2$ or 4). An equational basis is given for each such variety.

1. INTRODUCTION

In recent years a great deal of work has been done on decompositions of complete undirected graphs into collections of edge-disjoint cycles which partition the edge set of the graph; see the survey [7] for example. Most of this work is concerned with decompositions where the cycles are all of the same length m. An *m-cycle system of order n* is an ordered pair (V, C) where V is the vertex set of the complete undirected graph K_n and C is a set of m-cycles (cycles of length m) which induce a partition of the edge set of K_n. That is each edge occurs in exactly one cycle of C.

The necessary conditions for the existence of an m-cycle system of finite order n are (see [7])

(1) if $n > 1$ then $n \geq m$,
(2) n is odd and
(3) m divides $\frac{n(n-1)}{2}$.

[1]I wish to thank Dr. Sheila Oates-Williams for her supervision and assistance in the preparation of this paper and Professors C. C. Lindner and C. A. Rodger for their most helpful suggestions. I would also like to acknowledge the support of an A.R.C. grant used to help fund this research.

A pair of vertices is said to occur at distance d in an m-cycle whenever there is a path in the cycle containing precisely d edges that connects the two vertices. If an m-cycle system (V, C) has the additional property that for a fixed d, every pair of vertices of V occurs at distance d exactly once in C then the m-cycle system is said to be *d-perfect*. An m-cycle system that is d-perfect for each $d < \frac{m}{2}$ is called a *Steiner m-cycle system*.

Lemma 1.1. *It can be shown* [10] *that for all integers m, ($m \neq 1, 2$ or 4), there exists an integer n' such that for all integers $n > n'$ there exists a Steiner m-cycle system of order n provided the necessary conditions listed above are satisfied.*

In this paper we need to make a more general definitions in which our decompositions need only consist of closed trails instead of cycles. A closed trail differs from a cycle in that a closed trail is a closed walk with no repeated edges whereas a cycle is a closed walk with no repeated edges and no repeated vertices, see [2]. We also wish to consider decompositions in which the closed trails are not necessarily of the same length.

Definition 1.2. *For any finite m, we define an m-circuit to be a cyclically ordered m-tuple $(x_1, x_2, \ldots, x_m)$ which we use to represent the closed trail*

$$x_1, x_1x_2, x_2, x_2x_3, \ldots, x_m, x_mx_1, x_1.$$

The pair a and b is said to occur at distance d in the m-circuit $(x_1, x_2, \ldots, x_m)$ whenever there exists an i such that $\{a, b\} = \{x_i, x_{i+d}\}$ where $i + d$ is reduced modulo m. We define a circuit of infinite length to be a linearly ordered collection $(\ldots, x_{-2}, x_{-1}, x_0, x_1, x_2, \ldots)$ which represents an infinite trail

$$\ldots, x_{-2}x_{-1}, x_{-1}, x_{-1}x_0, x_0, x_0x_1, x_1, x_1x_2, \ldots.$$

As with the finite case, the pair a and b is said to occur at distance d in the infinite circuit $(\ldots, x_{-2}, x_{-1}, x_0, x_1, x_2, \ldots)$ whenever there exists an i such that $\{a, b\} = \{x_i, x_{i+d}\}$

It is worth noting that the pair $\{a, b\}$ occurs at distance 1 whenever the edge ab occurs.

Definition 1.3. *An L-circuit system of order n is an ordered pair (N, C) where N is a set of cardinality n and C is a set of circuits, whose lengths make up the set L, such that each unordered pair of distinct elements of N occurs exactly once at distance 1 in the circuits of C and no element of N occurs at distance 1 from itself.*

It is clear that an L-circuit system of order n represents a decomposition of the complete undirected graph K_n on a vertex set N of cardinality n into a set of closed trails, (and possibly some infinite trails) whose lengths make up the set L, which induces a partition of the edge set of K_n. In particular, any m-cycle system is represented by an $\{m\}$-circuit system in which each circuit consists entirely of distinct entries.

Definition 1.4. *An L-circuit system is said to be uniform if each circuit consists entirely of distinct entries.*

The condition that finite m-cycle systems have odd order applies to L-circuit systems as well.

Lemma 1.5. *Any finite L-circuit system (N, C) has odd order.*

Proof. Consider any element $a \in N$. Since each element other than a occurs at distance 1 from a once each and since there are two elements at distance 1 from a each time it occurs, the number off elements other than a must be even. Hence, the total number of elements in N must be odd. □

The m-cycle system property of being d-perfect can be defined similarly for L-circuit systems.

Definition 1.6. *An L-circuit system (N, C) is said to be d-perfect if for a fixed d each unordered pair of distinct elements of N occurs exactly once at distance d in the circuits of C and no element of N occurs at distance d from itself.*

In this paper we are concerned with 2-perfect L-circuit systems and a variety of quasigroups which they give rise to. A quasigroup (a set Q with one binary operation denoted by $\cdot$ which satisfies the condition that for any a and b in Q the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions for x and y in Q) is defined by universal algebraists as an algebra $\mathbf{Q} = \langle Q, \cdot, /, \backslash \rangle$ which satisfies the identities

(1) $(x \cdot y)/y = x$,
(2) $(x/y) \cdot y = x$,
(3) $y\backslash(y \cdot x) = x$ and
(4) $y \cdot (y\backslash x) = x$.

The three binary operations denoted by $\cdot, /$ and $\backslash$ are usually refered to as "multiplication","right division" and "left division" respectively. It is well known that the "multiplication table" of a quasigroup defines and is defined by a latin square. We find it necessary to use the "universal algebra" definition of a quasigroup so that the class of all quasigroups forms a variety.

For a formal definition of a variety see [4]. For our purposes the definition that the class of all algebras of the same type (by of the same type we mean they all have the same number of nullary operations, same number of unary operations, same number of binary operations etc) that satisfy a given collection of identities forms a variety is sufficient.

It is a well known result of Birkhoff that a class of algebras forms a variety if and only if it is closed under taking of subalgebras, cartesian products and homomorphic images, see [4].

It is worth noting at this point that if (N, C) is a 2-perfect L-circuit system then any element $a \in N$ can not occur at distance 4 from itself in C (neither can it occur at distance 1 or 2 from itself by definition). If a occurs at distance 4 from itself then there must be an element which occurs at distance 2 from a twice, which is impossible. Hence, since each element in a circuit of length l occurs at distance l from itself we can not have circuits of length 1, 2 or 4 in a 2-perfect L-circuit system.

2. QUASIGROUPS ARISING FROM 2-PERFECT L-CIRCUIT SYSTEMS

There is a well known method, see [7], for defining a quasigroup on the vertex set of the graph of any 2-perfect m-cycle system. This method works equally well for the more general case of 2-perfect L-circuit systems. Given any 2-perfect L-circuit system (N, C) we define two binary operations $*$ and $\circ$ on N as follows

(1) $a * a = a$ and $a \circ a = a$, for all $a \in N$ and
(2) for distinct a and b in N, $a * b = c$ and $a \circ c = b$ if and only if the ordered sequence a, b, c occurs within a circuit of C.

Since each pair of distinct elements of N occurs once at distance 1 and exactly once at distance 2 in C these two operations are well defined. It is straight forward to check that any algebra $\mathbf{N} = \langle N, *, \circ \rangle$ which we obtain in this manner from a 2-perfect L-circuit system (N, C) will satisfy the following of identities

(1) $x * x = x$
(2) $x \circ x = x$
(3) $(x * y) * y = x$
(4) $y * (y \circ x) = x$
(5) $y \circ (y * x) = x$

Definition 2.1. *The variety of all algebras* $\mathbf{N} = \langle N, *, \circ \rangle$ *satisfying the above five identities is called* $\mathcal{V}$.

If we define a set $\{\cdot, /, \backslash\}$ of three binary operations on the underlying set N of an algebra $\mathbf{N} \in \mathcal{V}$ as follows

(1) $a \cdot b = a * b$,
(2) $a/b = a * b$ and
(3) $a \backslash b = a \circ b$,

then it is easy to check that $\mathbf{N}$ satisfies the four quasigroup identities and hence is a quasigroup. Hence we may say that any $\mathbf{N} = \langle N, *, \circ \rangle \in \mathcal{V}$ is a quasigroup where "multiplication" and "right division" are both given by $*$ and "left division" is given by $\circ$. These quasigroups were first introduced in 1970 by A. Kotzig [5] and are called *partition quasigroups* or *P-quasigroups*.

To show that there is a one-one correspondence between $\mathcal{V}$ and the class of all 2-perfect L-circuit systems, we describe a method of constructing a 2-perfect L-circuit system (N, C) from any given algebra $\mathbf{N} \in \mathcal{V}$ such that when we define $*$ and $\circ$ on N in the above manner we get the algebra back again.

Before describing this method it is convenient to define a sequence of words $W_i(x, y)$, where i is any integer by

$$W_0(x, y) = x$$
$$W_1(x, y) = y$$
$$W_2(x, y) = x * y$$
$$W_3(x, y) = y * (x * y)$$

and inductively define $W_i(x,y) = W_{i-2}(x,y) * W_{i-1}(x,y)$. This gives us a well defined value for $W_i(x,y)$ when $i < 0$ since

$$W_{i-1}(x,y) = (W_{i-1}(x,y) * W_i(x,y)) * W_i(x,y) = W_{i+1}(x,y) * W_i(x,y).$$

Where there can be no confusion we sometimes just write W_i instead of $W_i(x,y)$.

Lemma 2.2. $W_i(W_j(x,y), W_{j+1}(x,y)) = W_{i+j}(x,y)$.

Proof. We use induction on i to prove this result. Let P_k be the proposition that $W_k(W_j, W_{j+1}) = W_{k+j}$. Let $k = 0$, then

$$W_k(W_j, W_{j+1}) = W_0(W_j, W_{j+1}) = W_j.$$

Hence, P_0 is true. Assume P_i is true for all $i \leq k$ and consider P_{k+1}.

$$\begin{aligned} & W_{k+1}(W_j, W_{j+1}) \\ =& W_{k-1}(W_j, W_{j+1}) * W_k(W_j, W_{j+1}) \\ =& W_{k+j-1} * W_{k+j} \\ =& W_{k+1+j} \end{aligned}$$

Hence, P_{k+1} is true and so P_k is true for all non-negative integers k. To show P_k is true for negative integers as well we need to show that if P_i is true for all $i \geq k$ then P_{k-1} is true.

$$\begin{aligned} & W_{k-1}(W_j, W_{j+1}) \\ =& (W_{k-1}(W_j, W_{j+1}) * W_k(W_j, W_{j+1})) * W_k(W_j, W_{j+1}) \\ =& W_{k+1}(W_j, W_{j+1}) * W_k(W_j, W_{j+1}) \\ =& W_{k+1+j} * W_{k+j} \\ =& (W_{k-1+j} * W_{k+j}) * W_{k+j} \\ =& W_{k-1+j} \end{aligned}$$

Hence, P_{k-1} is true and so P_k is true for all integers k. □

Given any $\langle N, *, \circ \rangle \in \mathcal{V}$ we construct a set C of circuits as follows. For each distinct a and b in N, if there exists a $t > 0$ such that $W_t(a,b) = a$ and $W_{t+1}(a,b) = b$ then we take the smallest such t and let

$$(W_0(a,b), W_1(a,b), W_2(a,b), \ldots W_{t-1}(a,b)) \in C.$$

If there does not exist such a t then we let the infinite circuit

$$(\ldots W_{-2}(a,b), W_{-1}(a,b), W_0(a,b), W_1(a,b), W_2(a,b), \ldots) \in C$$

The identity $(x * y) * y = x$ and the way we define the sequence of words W_i ensures that any distinct pair occurs at distance 1 exactly once (any circuit is uniquely determined by any pair it contains at distance 1). The existence of each distinct pair at distance 2 follows from the identity $y * (y \circ x) = x$ and uniqueness follows from $y \circ (y * x) = x$. The idempotent laws, (1) and (2) ensure that nothing occurs at distance 1 or 2 from itself (we note however that either of the idempotent laws can be deduced from the rest of the identities).

Definition 2.3. *The algebra* $\mathbf{Q}$ *corresponding to a 2-perfect L-circuit system* (Q, C) *is called an L-P-quasigroup and for brevity we refer to the circuits in the 2-perfect L-circuit system corresponding to the L-P-quasigroup* $\mathbf{Q}$ *simply as the circuits of* $\mathbf{Q}$. *If* $|L| = 1$, *say* $L = \{m\}$, *then we usually write just m-P-quasigroup instead of* $\{m\}$*-P-quasigroup.*

3. HOMOMORPHISMS OF P-QUASIGROUPS

Theorem 3.1. *If* $\mathbf{Q}$ *is the homomorphic image of an L-P-quasigroup* $\mathbf{P}$ *and there is a t-circuit in* $\mathbf{Q}$ *then there is an* $l \in L$ *such that t divides l.*

Proof. Let ϕ be a homomorphism from $\mathbf{P}$ onto $\mathbf{Q}$ and let $(x_0, x_1, \ldots, x_{t-1})$ be a circuit of $\mathbf{Q}$. Also, let $y_0 \in \phi^{-1}(x_0)$ and $y_1 \in \phi^{-1}(x_1)$ and let $(y_0, y_1, \ldots y_{l-1})$ be the circuit given by $\mathbf{P}$ that contains y_0 and y_1 at distance 1. Now, $W_l(y_0, y_1) = y_0$ and $W_{l+1}(y_0, y_1) = y_1$ and so since ϕ is a homomorphism, we must have

$$W_l(x_0, x_1) = W_l(\phi(y_0), \phi(y_1)) = \phi(y_0) = x_0$$

and

$$W_{l+1}(x_0, x_1) = W_{l+1}(\phi(y_0), \phi(y_1)) = \phi(y_1) = x_1.$$

Hence, t divides l. □

Theorem 3.2. *Let* $\mathbf{Q}$ *be an L-P-quasigroup in which each member of L divides a fixed integer m. Then there exists an m-P-quasigroup* $\mathbf{P}$ *of order* $|Q||N|$ *with a homomorphism onto* $\mathbf{Q}$ *if there is a set N such that*

(1) *there exists an m-P-quasigroup* $\mathbf{N} = \langle N, *, \circ \rangle$ *and*
(2) *for each* $l \in L$, *N can be partitioned into disjoint subsets each of size* $\frac{m}{l}$.

Proof. If $m = 3$ then clearly we can let $\mathbf{P} = \mathbf{Q}$ and we are finished. Hence, we may assume $m \geq 5$ and so if there is an m-P-quasigroup $\mathbf{N}$ then there exists a set of three mutually orthogonal latin squares defined on N since $|N| \notin \{2, 3, 6, 10\}$. There exists a set of three mutually orthogonal latin squares $\{L_1, L_2, L_3\}$ of side n for all n (including n infinite) except $n \in \{2, 3, 6\}$ and possibly $n = 10$, see [8] and [9].

For each positive integer i let $\langle N, *_i, /_i, \backslash_i \rangle$ be the quasigroup obtained from the latin square L_j where $i \equiv j \pmod 3$. Let D be the set of circuits of an m-P-quasigroup $\mathbf{N}$. Also, for each $l \in L$, partition N into disjoint subsets ${N^l}_s = \{x(l, s, 1), x(l, s, 2), \ldots, x(l, s, \frac{m}{l})\}$ where each $x(l, s, t) \in N$, ($l \in L, s \in S_l$ say, and $t \in \{1, 2, \ldots, \frac{m}{l}\}$) so that $N = \bigcup_{s \in S_l} {N^l}_s$. Hence, for any given $l \in L$ and $j \in N$ there is a unique $s \in S_l$ and a unique t such that $j = x(l, s, t)$, $(1 \leq t \leq \frac{m}{l})$.

Now, we define a set C of m-circuits whose entries are chosen from the set $Q \times N$ as follows. For each m-circuit $(y_1, y_2, \ldots, y_m) \in D$ and for each $i \in Q$ let $((i, y_1), (i, y_2), \ldots, (i, y_m)) \in C$.

Also, for each l, for each l-circuit $(x_1, x_2, \ldots, x_l)$ given by $\mathbf{Q}$, for each $s \in S_l$ and for each $j \in N$ let

$$((x_1,j),(x_2,x(l,s,1)),(x_3,x(l,s,1)*_3 j),\ldots,(x_l,x(l,s,1)*_l j),$$
$$(x_1,j),(x_2,x(l,s,2)),(x_3,x(l,s,2)*_3 j),\ldots,(x_l,x(l,s,2)*_l j),$$
$$(x_1,j),(x_2,x(l,s,3)),(x_3,x(l,s,3)*_3 j),\ldots,(x_l,x(l,s,3)*_l j),\ldots$$
$$\ldots,(x_1,j),(x_2,x(l,s,\frac{m}{l})),(x_3,x(l,s,\frac{m}{l})*_3 j),\ldots,(x_l,x(l,s,\frac{m}{l})*_l j))\in C$$

We now show that $(Q\times N, C)$ is a 2-perfect $\{m\}$-circuit system by showing that any pair of distinct elements (p,a) and (q,b) of $Q\times N$ occur exactly once at distance 1 and exactly once at distance 2 in C. Suppose $p=q$ and let $(y_1,y_2,\ldots,y_m)$ be the circuit in D in which a and b occur at distance 1(2). Then (p,a) and (q,b) occur at distance 1(2) only in the circuit $((p,y_1),(p,y_2),\ldots,(p,y_m))$ of C.

Now suppose $p\neq q$. We do distance 1 and 2 separately. First, for distance 1, let $(x_1,x_2,\ldots,x_l)$ be the unique circuit given by Q that contains p and q at distance 1. There are four cases to consider.

(1) $\{p,q\}=\{x_1,x_2\}$, without loss of generality suppose $p=x_1$ and $q=x_2$. Let $j=a$ and suppose $b=x(l,s,t)$. Then (p,a) and (q,b) occur at distance 1 only in the circuit

$$((x_1,j),(x_2,x(l,s,1)),\ldots,(x_1,j),(x_2,x(l,s,t)),\ldots).$$

(2) $\{p,q\}=\{x_1,x_l\}$, without loss of generality suppose $p=x_1$ and $q=x_l$. Let $j=a$ and choose the unique $x(l,s,t)$ such that $x(l,s,t)*_l j=b$. Then (p,a) and (q,b) occur at distance 1 only in the circuit

$$((x_1,j),(x_2,x(l,s,1)),\ldots,(x_l,x(l,s,t)*_l j),(x_1,j),\ldots).$$

(3) $\{p,q\}=\{x_2,x_3\}$, without loss of generality suppose $p=x_2$ and $q=x_3$. Suppose $a=x(l,s,t)$ and choose the unique j such that $x(l,s,t)*_3 j=b$. Then (p,a) and (q,b) occur at distance 2 only in the circuit

$$((x_1,j),(x_2,x(l,s,1)),\ldots,(x_2,x(l,s,t)),(x_3,x(l,s,t)*_3 j),\ldots).$$

(4) Neither p nor q is in $\{x_1,x_2\}$. In this case $p=x_\alpha$ and $q=x_\beta$ with

$$(x_1,x_2,\ldots,x_l)=(x_1,x_2,\ldots,x_\alpha,x_\beta\ldots,x_l)$$

or

$$(x_1,x_2,\ldots,x_l)=(x_1,x_2,\ldots,x_\beta,x_\alpha\ldots,x_l).$$

For each $u\in N$ choose w_u such that $u*_\alpha w_u=a$. Since $\langle N,*_\alpha,/_\alpha,\backslash_\alpha\rangle$ and $\langle N,*_\beta,/_\beta,\backslash_\beta\rangle$ are obtained from orthogonal latin squares, $\{u*_\beta w_u \mid u\in N\}=N$. Choose the unique $u\in N$ such that $u*_\beta w_u=b$, let $j=w_u$ and suppose $u=x(l,s,t)$.

Then (p,a) and (q,b) occur at distance 1 only in the circuit

$$((x_1,j),(x_2,x(l,s,1)),\ldots,(x_\alpha,x(l,s,t)*_\alpha j),(x_\beta,x(l,s,t)*_\beta j),\ldots)$$

or

$$((x_1,j),(x_2,x(l,s,1)),\ldots,(x_\beta,x(l,s,t)*_\beta j),(x_\alpha,x(l,s,t)*_\alpha j),\ldots).$$

Now for distance 2. Let $(x_1, x_2, \ldots, x_l)$ be the unique circuit given by Q in which p and q occur at distance 2. There are five cases to consider.

(1) $\{p, q\} = \{x_1, x_3\}$, without loss of generality suppose $p = x_1$ and $q = x_3$. Let $j = a$ and choose the unique $x(l, s, t)$ such that $x(l, s, t) *_3 j = b$. Then (p, a) and (q, b) occur at distance 2 only in the circuit

$$((x_1, j), (x_2, x(l, s, 1)), \ldots, (x_1, j), (x_2, x(l, s, t)), (x_3, x(l, s, t) *_3 j), \ldots).$$

(2) $\{p, q\} = \{x_1, x_{l-1}\}$, without loss of generality suppose $p = x_1$ and $q = x_{l-1}$. Let $j = a$ and choose the unique $x(l, s, t)$ such that $x(l, s, t) *_{l-1} j = b$. Then (p, a) and (q, b) occur at distance 2 only in the circuit

$$((x_1, j), (x_2, x(l, s, 1)), \ldots, (x_{l-1}, x(l, s, t) *_{l-1} j), (x_l, s_t *_l j), (x_1, j), \ldots).$$

(3) $\{p, q\} = \{x_2, x_4\}$, without loss of generality suppose $p = x_2$ and $q = x_4$. Suppose $a = x(l, s, t)$ and choose the unique j such that $x(l, s, t) *_4 j = b$. Then (p, a) and (q, b) occur at distance 2 only in the circuit

$$((x_1, j), (x_2, x(l, s, 1)), \ldots, (x_2, x(l, s, t)), (x_3, x(l, s, t) *_3 j), (x_4, x(l, s, t) *_4 j), \ldots).$$

(4) $\{p, q\} = \{x_2, x_l\}$, without loss of generality suppose $p = x_2$ and $q = x_l$. Suppose $a = x(l, s, t)$ and choose the unique j such that $x(l, s, t-1) *_l j = b$. Then (p, a) and (q, b) occur at distance 2 only in the circuit

$$((x_1, j), (x_2, x(l, s, 1)), \ldots (x_l, x(l, s, t-1) *_l j), (x_1, j), (x_2, x(l, s, t)), \ldots).$$

(5) Neither p nor q is in $\{x_1, x_2\}$. In this case $p = x_\alpha$ and $q = x_\beta$ with

$$(x_1, x_2, \ldots, x_l) = (x_1, x_2, \ldots, x_\alpha, x_\gamma, x_\beta \ldots, x_l)$$

or

$$(x_1, x_2, \ldots, x_l) = (x_1, x_2, \ldots, x_\beta, x_\gamma, x_\alpha \ldots, x_l).$$

For each $u \in N$ choose w_u such that $u *_\alpha w_u = a$. Since $\langle N, *_\alpha, /_\alpha, \backslash_\alpha \rangle$ and $\langle N, *_\beta, /_\beta, \backslash_\beta \rangle$ are obtained from orthogonal latin squares, $\{u *_\beta w_u \mid u \in N\} = N$. Choose the unique $u \in N$ such that $u *_\beta w_u = b$, let $j = w_u$ and suppose $u = x(l, s, t)$. Then (p, a) and (q, b) occur at distance 2 only in the circuit

$$((x_1, j), (x_2, x(l, s, 1)), \ldots$$
$$\ldots, (x_\alpha, x(l, s, t) *_\alpha j), (x_\gamma, x(l, s, t) *_\gamma j), (x_\beta, x(l, s, t) *_\beta j), \ldots)$$

or

$$((x_1, j), (x_2, x(l, s, 1)), \ldots$$
$$\ldots, (x_\beta, x(l, s, t) *_\beta j), (x_\gamma, x(l, s, t) *_\gamma j), (x_\alpha, x(l, s, t) *_\alpha j), \ldots).$$

It is straight forward to check that the map $\phi((p, a)) = p$ is a homomorphism from $\mathbf{P}$ (the m-P-quasigroup of $(Q \times N, C)$) onto $\mathbf{Q}$. $\square$

4. SUBVARIETIES AND RESTRICTIONS ON L

In this section we examine subvarieties of $\mathcal{V}$ whose members contain circuits, all of whose lengths divide a positive integer m, ($m \neq 1, 2$ or 4).

Definition 4.1. *For each positive integer m we define the subvariety $\mathcal{V}_m$ of $\mathcal{V}$ by the identity $W_m(x, y) = x$.*

Lemma 4.2. *If $\mathbf{Q}$ is an L-P-quasigroup where each $l \in L$ divides m then $\mathbf{Q} \in \mathcal{V}_m$.*

Proof. Let x_0 and x_1 be any two elements in Q and let $(x_0, x_1, x_2, \ldots, x_{l-1})$ be the l-circuit in $\mathbf{Q}$ which contains x_0 and x_1 at distance 1. Then, since l divides m we have $W_m(x_0, x_1) = x_0$. Hence, $\mathbf{Q} \in \mathcal{V}_m$. □

Lemma 4.3. *If $\mathbf{Q} \in \mathcal{V}_m$ then $\mathbf{Q}$ is an L-P-quasigroup where each $l \in L$ divides m.*

Proof. Let $(x_0, x_1, x_2, \ldots, x_{l-1})$ be a circuit of $\mathbf{Q}$ and let $m = tl + r$ where $0 \leq r \leq l - 1$. Then

$$\begin{aligned} x_0 &= W_m(x_0, x_1) \\ &= W_r(W_{tl}(x_0, x_1), W_{tl+1}(x_0, x_1)) \\ &= W_r(x_0, x_1) \end{aligned}$$

and

$$\begin{aligned} x_1 &= W_1(x_0, x_1) \\ &= W_m(W_1(x_0, x_1), W_2(x_0, x_1)) \\ &= W_r(W_{tl+1}(x_0, x_1), W_{tl+2}(x_0, x_1)) \\ &= W_{r+1}(W_{tl}(x_0, x_1), W_{tl+1}(x_0, x_1)) \\ &= W_{r+1}(x_0, x_1). \end{aligned}$$

Hence, if $r \neq 0$ then we have x_0 and x_1 occurring twice at distance 1 which is impossible and so $r = 0$ and l divides m. □

These last two lemmata tell us that $\mathcal{V}_m$ must consist precisely of those L-P-quasigroups in which each member of L divides m. We note that for each m, ($m \neq 1, 2$ or 4) the trivial L-P-quasigroup of order 1 (here $L = \emptyset$) is in $\mathcal{V}_m$.

Definition 4.4. *The class of all m-P-quasigroups is called C_m.*

Theorem 4.5. *The variety $\mathcal{V}_m$ is generated by C_m.*

Proof. Let $\mathbf{Q} \in \mathcal{V}_m$. We will show using Theorem 3.2 that there exists a $\mathbf{P} \in C_m$ with a homomorphic image onto $\mathbf{Q}$. We only need to show that a set N satisfying the two conditions of Theorem 3.2 exists. Any countably infinite set will do (the conditions under which a finite set N exists are considered in Section 6). Clearly, any countably infinite set satisfies condition (2) and (one way) we can obtain a countably infinite m-P-quasigroup is by taking the cartesian product of a countably infinite number of copies of any finite m-P-quasigroup (which exists by Lemma 1.1). □

5. UNIFORM P-QUASIGROUPS

Definition 5.1. *A uniform L-P-quasigroup is an L-P-quasigroup whose circuits consist entirely of distinct elements.*

We note that this definition is consistent with Definition 1.4 in that uniform L-P-quasigroups correspond to uniform 2-perfect L-circuit systems.

Definition 5.2. *The class of all uniform m-P-quasigroups is called* $\mathcal{U}_m$.

We will now show that $\mathcal{V}_m$ is generated by $\mathcal{U}_m$. Since we already know that $\mathcal{V}_m$ is generated by $\mathcal{C}_m$ it is sufficient to prove the following theorem.

Theorem 5.1. *Let* $\mathbf{Q}$ *be an m-P-quasigroup then there exists a uniform m-P-quasigroup* $\mathbf{P}$ *such that there is a homomorphism from* $\mathbf{P}$ *onto* $\mathbf{Q}$.

Proof. Let (N, D) be a finite uniform 2-perfect m-circuit system where $|N| \neq 3$ (such a system exists for all $m \neq 1, 2$ or 4 by Lemma 1.1). We may assume $N = \{1, 2, \ldots, n\}$ where $n = |N|$. Then as we remarked in the proof of Theorem 3.2, there exists a set of three mutually orthogonal latin squares L_1, L_2 and L_3 of side n. As before, for each positive integer i we define $\langle N, *_i, /_i, \backslash_i \rangle$ to be the quasigroup obtained from the latin square L_j where $i \equiv j \pmod 3$.

We now construct a set of $k = \frac{m(m-5)}{2}$, $n^2 \times m$ arrays with entries chosen from N. For each of the k pairs of integers (a, b) with $a, b \in \{1, 2, \ldots, m\}, a < b$ and a and b not at distance 1 or 2 in the circuit $(1, 2, \ldots, m)$, we define the array A_{ab} as follows.

For each of the n^2 ordered pairs $(i, j) \in N \times N$ make

$$(i *_1 j, i *_2 j, \ldots, i *_{a-1} j, i, i *_{a+1} j, \ldots, i *_{b-1} j, i + 1, i *_{b+1} j, \ldots, i *_m j)$$

a row of the array A_{ab} (of course if $i = n$ then we reduce $i + 1$ modulo n to 1). Hence we have a collection of arrays

$$A_{a_0 b_0}, A_{a_1 b_1}, A_{a_2 b_2}, \ldots, A_{a_{k-1} b_{k-1}}, \qquad (\text{where } k = \frac{m(m-5)}{2})$$

Each array A_{ab} then has the following properties. Firstly, in any row the entries in columns a and b are distinct (this is clear since the entries in these columns are i and $i+1$). Secondly, if you run your fingers down any pair of columns say column c and column d where c and d are at distance 1 or 2 in the circuit $(1, 2, \ldots, m)$, then you get each of the n^2 ordered pairs in $N \times N$ once each. To see this we consider the two possible cases,

(1) One of c and d, say c, is in $\{a, b\}$ (since a and b are not at distance 1 or 2 in $(1, 2, \ldots, m)$ we can not have both c and d in $\{a, b\}$).

If a pair occurs twice when you run your fingers down these two columns then we must have $i *_d j_1 = i *_d j_2$ for distinct j_1 and j_2, which is impossible since $\langle N, *_d, /_d, \backslash_d \rangle$ is a quasigroup.

(2) Neither c nor d is in $\{a, b\}$.

If a pair occurs twice when you run your fingers down these two columns then we must have $i_1 *_c j_1 = i_2 *_c j_2$ and $i_1 *_d j_1 = i_2 *_d j_2$ where $(i_1, j_1) \neq (i_2, j_2)$, which is impossible since $\langle N, *_c, /_c, \backslash_c \rangle$ and $\langle N, *_d, /_d, \backslash_d \rangle$ are obtained from orthogonal latin squares.

Let $R_0 = Q$ (the underlying set of $\mathbf{Q}$) and for $i = 0, 1, \ldots, k-1$ let $R_{i+1} = R_i \times N$. We now construct a sequence of sets of m-circuits $C_0, C_1, C_2, \ldots, C_k$ with entries chosen from $R_0, R_1, R_2, \ldots, R_k$ respectively, by using the collection of arrays, the uniform m-circuit system (N, D) and the m-circuit system (R_0, C_0) corresponding to $\mathbf{Q}$.

We construct C_{t+1} from C_t as follows.

For each m-circuit $(x_1, x_2, \ldots, x_m) \in C_t$ and for each row $(y_1, y_2, \ldots, y_m)$ of the array $A_{a_t b_t}$ let

$$((x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)) \in C_{t+1}.$$

Also, for each $a \in R_t$ and for each distinct m-circuit $(z_1, z_2, \ldots, z_m) \in D$ let

$$((a, z_1), (a, z_2), \ldots, (a, z_m)) \in C_{t+1}.$$

We show by induction on i that each collection C_i forms an m-circuit system (R_i, C_i) with the property that any m-circuit in C_i has distinct entries in positions a_j and b_j for each $j \leq i - 1$.

Firstly, it is clear that C_0 has this property so we assume that (R_i, C_i) is an m-circuit system with the property and we show that (R_{i+1}, C_{i+1}) is an m-circuit system with the property. Let (p_1, q_1) and (p_2, q_2) be any two distinct elements of R_{i+1}. If $p_1 = p_2$, then (p_1, q_1) and (p_2, q_2) occur at distance 1(2) only in the m-circuit

$$((a, z_1), (a, z_2), \ldots, (a, z_m)),$$

where $a = p_1 = p_2$ and $(z_1, z_2, \ldots, z_m)$ is the unique m-circuit in D in which q_1 and q_2 occur at distance 1(2).

If $p_1 \neq p_2$, then the pair p_1 and p_2 must occur at distance 1(2) in exactly one m-circuit $(x_1, x_2, \ldots, x_m) \in C_i$ say $p_1 = x_{p'_1}$ and $p_2 = x_{p'_2}$. Hence, (p_1, q_1) and (p_2, q_2) occur at distance 1(2) only in the m-circuit $((x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k))$, where $(y_1, y_2, \ldots, y_k)$ is the row in the array $A_{a_i b_i}$ which contains q_1 and q_2 in columns p'_1 and p'_2. Since $x_{p'_1}$ and $x_{p'_2}$ are at distance 1(2) in $(x_1, x_2, \ldots, x_m)$ there exists a unique row with this property.

We now show that any m-circuit in C_{i+1} has distinct entries in positions a_j and b_j for each $j \leq i$. Firstly, the circuit $(z_1, z_2, \ldots, z_m)$ belongs to a uniform P-circuit m-design and so each $((a, z_1), (a, z_2), \ldots, (a, z_m))$ consists entirely of distinct entries.

Also, any $((x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m))$ has distinct entries in positions a_j and b_j for each $j \leq i$ because the first coordinates are distinct in the positions a_j and b_j for $j \leq i - 1$ and the second coordinates are distinct in positions a_i and b_i by the properties of the array. Hence, by induction, each (R_i, C_i) is an m-circuit system with the property. So each m-circuit in C_k consists entirely of distinct entries and hence is a uniform m-circuit system.

We show that if $\mathbf{P}$ is the uniform m-P-quasigroup corresponding to (R_k, C_k), then there is a homomorphism from $\mathbf{P}$ onto $\mathbf{Q}$. For each $i \in \{1, 2, \ldots, k\}$ we define a map ϕ_i from the m-P-quasigroup $\mathbf{Q}_i$ corresponding to (R_i, C_i) onto the m-P-quasigroup $\mathbf{Q}_{i-1}$ corresponding to (R_{i-1}, C_{i-1}) by $\phi_i((a, b)) = a$. It is easy to see that for each i, ϕ_i is onto and ϕ_i preserves the three binary operations. Hence the map $\phi = \phi_1\phi_2 \ldots \phi_{k-1}\phi_k$ is a homomorphism from $\mathbf{P} = \mathbf{Q}_k$ onto $\mathbf{Q} = \mathbf{Q}_0$. □

6. FINITE P-QUASIGROUPS

Earlier, in order to show that $\mathcal{C}_m$ generates $\mathcal{V}_m$, we constructed for any $\mathbf{Q} \in \mathcal{V}_m$ an infinite m-P-quasigroup which had a homomorphism onto $\mathbf{Q}$. In this section we look at the conditions under which it is possible, given a finite $\mathbf{Q} \in \mathcal{V}_m$, to find a finite m-P-quasigroup which has a homomorphism onto $\mathbf{Q}$. If it is possible then Theorem 5.1 tells us that there exists a finite uniform m-P-quasigroup which has a homomorphism onto $\mathbf{Q}$.

Theorem 6.1. *Let $\mathbf{Q}$ be an L-P-quasigroup and suppose there is a homomorphism from a finite P-quasigroup $\mathbf{P}$ onto $\mathbf{Q}$. Then, for each $l \in L$ there is a circuit of length lr, where r is odd, in $\mathbf{P}$.*

Proof. Let $(x_1, x_2, \ldots, x_l)$ be an l-circuit of $\mathbf{Q}$ and for each $i \in \{1, 2, \ldots, l\}$ let $X_i = \phi^{-1}(x_i)$ where ϕ is a homomorphism from $\mathbf{P}$ onto $\mathbf{Q}$ so that each X_i is a congruence class of the congruence on $\mathbf{P}$ induced by ϕ. Since $\mathbf{P}$ is idempotent in each of its binary operations it is clear that each $\mathbf{X}_i = \langle X_i, *, \circ \rangle$ is itself a P-quasigroup and so $|X_i|$ is odd.

Let $E_i = X_i \times X_{i+1}$ (of course, $X_{l+1} = X_1$). Now, it is well known (see [4]) that quasigroups have uniform congruences (that is each congruence class has the same cardinality) and so we have $|X_1| = |X_2| = \cdots = |X_l| = t$ say where t is odd. Hence, $|E_1 \cup E_2 \cup \cdots \cup E_l| = lt^2$. Now, since $\mathbf{P}$ is finite, for any $(y_i, y_{i+1}) \in E_i$ there exists a smallest integer s_1 such that $W_{s_1}(y_i, y_{i+1}) = y_i$ and $W_{s_1+1}(y_i, y_{i+1}) = y_{i+1}$. Hence, since ϕ is a homomorphism,

$$\begin{aligned} W_{s_1}(x_i, x_{i+1}) &= W_{s_1}(\phi(y_i), \phi(y_{i+1})) \\ &= \phi(W_{s_1}(y_i, y_{i+1})) \\ &= \phi(y_i) \\ &= x_i \end{aligned}$$

and

$$\begin{aligned} W_{s_1+1}(x_i, x_{i+1}) &= W_{s_1+1}(\phi(y_i), \phi(y_{i+})) \\ &= \phi(W_{s_1+1}(y_i, y_{i+1})) \\ &= \phi(y_{i+1}) \\ &= x_{i+1}. \end{aligned}$$

Hence, l divides s_1. If we now select another pair $(y_{i'}, y_{i'+1})$ in $E_{i'}$ say , which does not appear at distance 1 in the s_1-circuit given above, then again there exists

a smallest integer s_2 such that $W_{s_2}(y_{i'}, y_{i'+1}) = y_{i'}$ and $W_{s_2+1}(y_{i'}, y_{i'+1}) = y_{i'+1}$ and as before l divides s_2.

By repeating this process until all the elements of $E_1 \cup E_2 \cup \cdots \cup E_l$ are used up we see that $|E_1 \cup E_2 \cup \cdots \cup E_l| = s_1 + s_2 + \cdots + s_w$. Hence, $lt^2 = l(a_1 + a_2 + \cdots + a_w)$, where $s_j = la_j$, and so $a_1 + a_2 + \cdots + a_w = t^2$ which is odd. Hence, there must be an odd integer $r \in \{a_1, a_2, \ldots, a_w\}$ and so there is a circuit of length lr, with r odd, in $\mathbf{P}$. $\square$

This theorem tells us that if there exists a finite m-P-quasigroup $\mathbf{P}$ (where $m = 2^t a$ with a odd) with a homomorphic image onto an L-P-quasigroup then we must necessarily have for each $l_i \in L$, $l_i = 2^t a_i$ where a_i is odd and a_i divides a. Let $m = 2^t a$ with a odd, and suppose $l_i = 2^{t_i} a_i$ with a_i odd. Then by Theorem 3.1, l_i divides m and so a_i must divide a. But, by Theorem 6.1, $m = 2^{t_i} a_i r_i$ where r_i is odd. Hence, $t_i = t$.

We will now show that these necessary conditions are also sufficient to ensure the existence of a finite m-P-quasigroup with a homomorphism onto any given finite L-P-quasigroup.

Lemma 6.2. *If $m = 2^t a$ ($m \neq 1, 2$ or 4) where a is odd then there exists an m-uniform P-quasigroup of order $n < \infty$ such that a divides n.*

Proof. Let the binary expression for a be $a = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_1 2 + 1$. We then choose $b = b_s 2^s + b_{s-1} 2^{s-1} + \cdots + b_1 2 + 1$ such that $ab > n'$ where the necessary existence conditions for uniform m-P-quasigroups of order n are sufficient for $n > n'$ (see Lemma 1.1) and

$$\begin{aligned} a_1 + b_1 &= 0 \\ a_2 + a_1 b_1 + b_2 &= 0 \\ a_3 + a_2 b_1 + a_1 b_2 + b_3 &= 0 \\ &\vdots \\ a_{t-1} + a_{t-2} b_1 + \cdots + b_{t-1} &= 0 \\ a_t + a_{t-1} b_1 + \cdots + b_t &= 0. \end{aligned}$$

Here, if $t > r$ then $a_{r+1}, a_{r+2}, \ldots, a_t = 0$. Clearly it is possible to choose such a b. Now, let $n = ab = (a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_1 2 + 1)(b_s 2^s + b_{s-1} 2^{s-1} + \cdots + b_1 2 + 1) = c_{r+s} 2^{r+s} + \cdots + c_{t+1} 2^{t+1} + 1$. Hence, 2^{t+1} divides $n - 1$ and so m divides $\frac{n(n-1)}{2}$. Hence, there exists a uniform m-P-quasigroup of order n such that a divides n. $\square$

Theorem 6.3. *For any given finite L-P-quasigroup $\mathbf{Q}$, there exists a finite m-P-quasigroup which has a homomrphism onto $\mathbf{Q}$ if and only if there is a fixed t such that*

(1) *$l_i = 2^t a_i$ for each $l_i \in L$,*
(2) *$m = 2^t a$ where a is odd and*
(3) *each a_i divides a.*

Proof. The "only if" part of the theorem follows immediately from Theorem 6.1. Conversely, let $\mathbf{Q}$ be a $\{2^t a_1, 2^t a_2, \ldots, 2^t a_k\}$-P-quasigroup and suppose each a_i divides an odd integer a. Then, by Lemma 6.2 there exists an m-P-quasigroup $\mathbf{G}$ (in fact there exists a uniform m-P-quasigroup) where $m = 2^t a$, of order $v < \infty$ such that a divides v.

Then the underlying set G of $\mathbf{G}$ is a set satisfying the two conditions of Theorem 3.2. Condition (1) is clearly satisfied. Condition (2) is also satisfied since a divides v implies $\frac{a}{a_i}$ divides v and so for each l_i, G can be partitioned into disjoint subsets each of size $\frac{m}{l_i} = \frac{2^t a}{2^t a_i} = \frac{a}{a_i}$.

Hence, by Theorem 3.2, there exists an m-P-quasigroup $\mathbf{P}$ of order $v|Q|$ (which is finite) such that there is a homomorphism from $\mathbf{P}$ onto $\mathbf{Q}$. □

7. COMMENTS AND QUESTIONS

(1) What is the variety generated by the finite members of $\mathcal{U}_m$? In particular if $m = 2^t a$ with a odd, is there a P-quasigroup with a circuit whose length is not of the form $2^t a_i$ with a_i dividing a in the variety generated by the finite members of $\mathcal{U}_m$? For example, consider $m = 6$. Do the 6-P-quasigroups which have homomorphic maps onto P-quasigroups with circuits of length 3 (these 6-P-quasigroups must be infinite by Theorem 6.1) belong to the variety generated by the finite 6-P-quasigroups ?

(2) Is the variety generated by $\mathcal{V}_{m_1}$ and $\mathcal{V}_{m_2}$ equal to $\mathcal{V}_m$ where m is the lowest common multiple of m_1 and m_2 ? For example consider the variety $\mathcal{V}_{3,5}$ generated by $\mathcal{V}_3$ and $\mathcal{V}_5$. Is $\mathcal{V}_{3,5}$ equal to $\mathcal{V}_{15}$ or does there exist a proper subvariety of $\mathcal{V}_{15}$ which contains both $\mathcal{V}_3$ and $\mathcal{V}_5$?

(3) For $m = 3, 5$ and 7 an equational base has been given for the class of quasigroups arising from all 2-perfect m-cycle systems ($\mathcal{U}_m$), see [**6**]. In [**6**] (and elsewhere) the question of whether or not there is an equational base for other values of m (in particular $m = 6$) is asked. The fact that $\mathcal{U}_m$ generates $\mathcal{V}_m$ tells us that $\mathcal{U}_m$ can not be equationally defined unless $\mathcal{U}_m = \mathcal{V}_m$ (this is the case for $m = 3, 5$ and 7 since for these values of m all m-P-quasigroups must be uniform because any repeat would necessarily be at distance 1, 2 or 4 from itself, which is not possible).

Hence, for all composite values of m, ($m \neq 1, 2$ or 4) except possibly $m = 8$ (8 is the only possible exception because it is the only composite integer, other than 1, 2 and 4, which has no proper factor other than 1, 2 and 4), $\mathcal{U}_m$ can not be equationally defined. This result has been proved previously by the author for $m = 6$ and for m odd and composite in [**3**].

Shown on the next page are the circuits of an 8-P-quasigroup of order 17 which is not uniform. This system was constructed by Peter Adams with similar techniques to those used in [**1**]. Hence, $\mathcal{U}_8 \neq \mathcal{V}_8$ and so $\mathcal{U}_8$ can not be equationally defined. This only leaves the question, for what values of m with m prime and greater than 7 do there exist m-P-quasigroups which are not uniform? For these values of m the class $\mathcal{U}_m$ can be equationally defined if and only if no non-uniform m-P-quasigroups exist.

0	1	9	4	14	0	15	11
1	2	10	5	15	1	16	12
2	3	11	6	16	2	0	13
3	4	12	7	0	3	1	14
4	5	13	8	1	4	2	15
5	6	14	9	2	5	3	16
6	7	15	10	3	6	4	0
7	8	16	11	4	7	5	1
8	9	0	12	5	8	6	2
9	10	1	13	6	9	7	3
10	11	2	14	7	10	8	4
11	12	3	15	8	11	9	5
12	13	4	16	9	12	10	6
13	14	5	0	10	13	11	7
14	15	6	1	11	14	12	8
15	16	7	2	12	15	13	9
16	0	8	3	13	16	14	10

REFERENCES

1. Adams P. and Billington E. J., *The spectrum for 2-perfect 8-cycle systems*, Ars Combin. (to appear).
2. Bondy J. A. and Murty U. S. R., *Graph theory with applications*, Macmillan, London, 1976, pp. 12-14.
3. Bryant D. E., *Varieties of quasigroups arising from 2-perfect m-cycle systems*, Designs, Codes and Cryptography **2** (1992), 159-168.
4. Evans T., *Varieties of loops and quasigroups*, Quasigroups and loops: theory and applications, Sigma Ser. Pure Math. 8, 1990, pp. 1-26.
5. Kotzig A., *Groupoids and partitions of complete graphs*, Combinatorial structures and their applications (Proc. Calgary Internat. Conf., Calgary, Alta), 215-221, Gordon and Breach, New York.
6. Lindner C. C., *Graph decompositions and quasigroup identities*, Proceedings of the Second International Catania Combinatorial Conference, *Graphs, designs and combinatorial geometries*, Universita di Catania, Catania, Sicily, September 4-9, 1989. Le Matematiche **XLV** (1990), 83-118.
7. Lindner C. C. and Rodger C. A., *Decomposition into cycles II: Cycle systems*, Contempory design theory: a collection of surveys, (J. H. Dinitz and D. R. Stinson, eds.), John Wiley and Sons (to appear).
8. Todorov D. T., *Three mutually orthogonal latin squares of order 14*, Ars Combin. **20** (1985), 45-47.
9. Wallis W. D., *Three orthogonal latin squares*, Adv. in Math (Beijing) **15** (1986), no. 3, 269-281.
10. Wilson R. M., Private Communication.

(Received 22/1/92)