COLLOQUIUM MATHEMATICUM

VOL. XLIII 1980 FASC. 1

ON THE CONSTRUCTION OF CYCLIC QUADRUPLE SYSTEMS

BY

K. T. PHELPS (ATLANTA, GEORGIA)

1. Introduction. A *Steiner quadruple system* of order n is a pair (Q, q) where Q is an n-set and q is a collection of 4-element subsets of Q, usually called *blocks*, such that every 3-element subset of Q is contained in exactly one block of q. Hanani [2] has proved that a Steiner quadruple system of order n, or briefly SQS(n), exists if and only if $n \equiv 2$ or $4 \pmod 6$. In the excellent survey of Steiner quadruple systems, Lindner and Rosa [4] raise a series of questions. This note is intended to answer two of them, concerning cyclic SQS(n).

An SQS(n) is called *cyclic* if it has an automorphism consisting of a single cycle of length n. If (Q, q) is a cyclic SQS(n) with cyclic automorphism $(0, 1, 2, \ldots, n-1)$, then with each block $\{x, y, z, w\}$ of q $(x < y < z < w)$ one can associate a (cyclically ordered) quadruple of differences (a, b, c, d), where $a = y-x$, $b = z-y$, $c = w-z$, $d = x-w \pmod n$. Lindner and Rosa [4] call a quadruple of differences *symmetric* if either

$$a = c \quad (\text{or } b = d)$$

or

$$a = b \text{ and } c = d \quad (\text{or } b = c \text{ and } d = a).$$

Then a cyclic SQS is said to be *S-cyclic* if all of its difference quadruples are symmetric. Finally, it is stated that all known cyclic SQS are *S*-cyclic [4]. One purpose of this paper then is to construct a cyclic SQS that is not *S*-cyclic. In particular, we construct one of order 20, thereby showing that there are at least two non-isomorphic cyclic SQS(20) (Question 5.1 in [4]). A secondary purpose is to establish some sufficient conditions for a cyclic SQS(n) to exist.

2. Constructions of Steiner quadruple systems. A *3-quasigroup of order n* is a pair $(P, \langle , , \rangle)$, where P is an n-set and $\langle , , \rangle$ is a ternary operation on P such that if any 3 of the terms in the equation $\langle x, y, z\rangle = w$ are given, then the fourth is uniquely determined. A 3-quasigroup is said

to be *commutative* if, for all $x, y, z \in P$,

$$\langle x, y, z\rangle = \langle x, z, y\rangle = \langle z, y, x\rangle = \langle y, x, z\rangle.$$

It is said to be *idempotent* if $\langle x, x, x\rangle = x$ for all $x \in P$ and *diagonalized* if, for any x, y, $\langle x, x, x\rangle = \langle y, y, y\rangle$ implies $x = y$. On a commutative 3-quasigroup $(P, \langle , , \rangle)$ we state the following conditions:

(a) for all $x, y \in P$, if $\langle x, x, y\rangle = z$ and $\langle x, y, y\rangle = w$, then

$$\{\langle z, z, w\rangle, \langle z, w, w\rangle\} = \{x, y\};$$

(b) for all ordered pairs (x, y), if $\langle x, x, y\rangle = u$ and $\langle u, u, x\rangle = v$, then

$$\langle v, v, u\rangle = y \quad \text{and} \quad \langle y, y, v\rangle = x.$$

LEMMA 1. *A commutative 3-quasigroup of order n that satisfies condition* (a) *can exist only if* $n \equiv 1$ *or* 2 (mod 3).

Proof. Let $(P, \langle , , \rangle)$ be a 3-quasigroup that is commutative and satisfies (a). Define a groupoid on P by $x*y = \langle x, x, y\rangle$ (and $y*x = \langle y, y, x\rangle$). Then the groupoid $(P, *)$ will be self-orthogonal (because of (i)), and thus it must be diagonalized. If $(P, *)$ is diagonalized, then, clearly, so must be $(P, \langle , , \rangle)$. However, since $(P, \langle , , \rangle)$ is commutative, the number of times an element occurs off the diagonal must be divisible by 3. Hence $n \equiv 1$ or 2 (mod 3).

We remark that this necessary condition on n is not sufficient. The author has determined, using a computer, that there exists no one of order 7. In the previous paper [5] the author proved the following results concerning these 3-quasigroups:

LEMMA 2 [5]. *There exists a commutative and idempotent 3-quasigroup that satisfies* (a) *for all orders* $n \equiv 2$ *or* 4 (mod 6) *and* $n = 5^t$ *for* $t \geqslant 1$.

LEMMA 3 [5]. *Given a commutative 3-quasigroup $(P, \langle , , \rangle)$ of order p that satisfies* (a), *one can construct an* SQS$(2p)$ (Q, q) *as follows*:

(1) $Q = P \times \{0, 1\}$;

(2) *for all triples* $\{x, y, z\} \subseteq P$,

$$\{x_i, y_i, z_i, \langle x, y, z\rangle_{i+1}\} \in q \quad \text{for } i = 0, 1$$

(*with the subscripts reduced* mod 2);

(3) *for all pairs* $x, y \subseteq P$,

$$\{x_0, y_0, \langle x, x, y\rangle_1, \langle y, y, x\rangle_1\} \in q.$$

A 3-quasigroup of order p is said to be *cyclic* if it has an automorphism that consists of a single cycle of length p. Then, as an immediate corollary to Lemma 3, we have

COROLLARY 1. *If there exists a cyclic 3-quasigroup of order p, $p \equiv 1 \pmod 2$, that is commutative and satisfies condition* (a), *then there exists a cyclic* SQS($2p$).

Note that the construction in Lemma 3 is in effect a generalization of a construction originally due to Doyen and Vandensavel [1] (i.e., Construction 2 and Problem 4.11).

LEMMA 4. *There exists a commutative, idempotent 3-quasigroup that satisfies conditions* (a) *and* (b) *for all orders n, $n \equiv 2$ or $4 \pmod 6$ and $n = 5^t$.*

Proof. The 3-quasigroups constructed in Lemma 2 satisfy condition (b) as well. For $n \equiv 2$ or $4 \pmod 6$, there exists a commutative 3-quasigroup that satisfies the identity $\langle x, x, y\rangle = y$ (generalized idempotent), and thus will satisfy (a) and (b). For $n = 5^t$, one can construct examples using GF(5^t), that is $\langle x, y, z\rangle = 2(x+y+z)$ (see [5]).

Next we present another construction of SQS.

LEMMA 5. *Given a commutative, idempotent 3-quasigroup $(P, \langle,,\rangle)$ that satisfies* (a) *and* (b), *one can construct an* SQS (Q, q) *as follows*:

(1) $Q = P \times \{0, 1, 2, 3\}$;

(2) *for all triples* $\{x, y, z\} \subseteq P$,

$$\{x_i, y_i, z_i, \langle x, y, z\rangle_{i+2}\} \in q, \quad i = 0, 1, 2, 3;$$

(3) *for all pairs* $\{x, y\} \subseteq P$,

$$\{x_i, y_i, \langle x, x, y\rangle_{i+2}, \langle x, y, y\rangle_{i+2}\} \in q, \quad i = 0, 1, 2, 3;$$

(4) *for all pairs* $\{x, y\} \subseteq P$ *and all* $z \in P$,

$$\{x_i, y_i, z_{i+1}, \langle x, y, z\rangle_{i+3}\} \in q, \quad i = 0, 1, 2, 3;$$

(5) *for all ordered pairs* (x, y) *with* $x, y \in P$, *where* $\langle x, x, y\rangle = z$ *and* $\langle z, z, x\rangle = w$, *we have* $\{x_0, y_1, z_3, w_2\} \in q$;

(6) $\{x_0, x_1, x_2, x_3\} \in q$ *for all* $x \in P$.

Note that in cases (2)-(6) subscripts are reduced mod 4 as necessary.

Proof. If $|P| = p$, then the total number of blocks from (2)-(6) is

$$4\binom{p}{3} + 2\binom{p}{2} + 4p\binom{p}{2} + 2\binom{p}{2} + p = \frac{4p(4p-1)(4p-2)}{4!}.$$

Since this is the right number of blocks for an SQS($4p$), all we need to do is to show that every triple occurs at least once.

Case (i). All triples of the form $\{x_i, y_i, z_i\}$ will occur in a block of type (2).

Case (ii). All triples of the form $\{x_i, y_i, z_{i+j}\}$ for $j = 1, 2, 3$ will occur in blocks of type (2), (3) or (4). For $j = 1$, this is obvious. For $j = 3$, from the fact that $(P, \langle, ,\rangle)$ is a 3-quasigroup it follows that blocks of this form will occur. In the case of $j = 2$, property (a) assures this (as in Lemma 3).

Case (iii). Triples of the form $\{x_i, y_{i+1}, z_{i+3}\}$ will occur in blocks of type (4) or (5), since there exists a w such that $\langle x, w, y\rangle = z$. If $w \neq x$, then, clearly, it will occur in some block of type (4). Otherwise, it will occur in a block of type (5). Property (b) assures this. If $\langle x, x, y\rangle = z$ and $\langle z, z, x\rangle = w$, then $\langle w, w, z\rangle = y$ and $\langle y, y, w\rangle = x$. Thus $\{x_0, y_1, z_3, w_2\} \in q$ by construction, but then so is $\{x_1, y_2, z_0, w_3\}$, since $\langle z, z, x\rangle = w$ and $\langle w, w, z\rangle = y$. In a similar manner one can show that

$$\{x_2, y_3, z_1, w_0\} \in q \quad \text{and} \quad \{x_3, y_0, z_2, w_1\} \in q.$$

Thus we conclude that $\{x_i, y_{i+1}, z_{i+3}\} \in q$ for $i = 0, 1, 2, 3$.

Case (iv). All triples of the form $\{x_i, x_j, x_k\}$, obviously, occur in blocks of type (6).

COROLLARY 2. *The* SQS *constructed in Lemma* 2.5 *will all have the automorphism* $x_i \to x_{i+1}$ *with the subscripts reduced* mod 4.

This is obvious from construction except for blocks of type (5). For these blocks, case (iii) gives us the result.

THEOREM 1. *If there exists a cyclic* 3*-quasigroup of order* p, $p \equiv 1 \pmod 2$, *that is commutative and idempotent and satisfies conditions* (a) *and* (b), *then there exists a cyclic* SQS$(4p)$.

This follows from Lemma 5 and Corollary 2.

We have established some sufficient conditions for a cyclic SQS(n) to exist. To be of interest, we should show that they are not vacuous.

COROLLARY 3. *There exists a cyclic* 3*-quasigroup of order* 5 *that is commutative, idempotent and satisfies conditions* (a) *and* (b). *Hence there exist a cyclic* SQS(10) *and a cyclic* SQS(20).

For the proof, let $P = \{0, 1, 2, 3, 4\}$ and

$$\langle x, y, z\rangle = 2(x+y+z) \pmod 5 \quad \text{for } x, y, z \in P.$$

3. Cyclic SQS(20). The cyclic SQS(20) constructed above (Corollary 3) contains subsystems of order 10. Hence it is not isomorphic to the S-cyclic SQS(20) constructed by Jain [3] (see [4]). Furthermore, it is easy to see that it is not S-cyclic. The base blocks for our cyclic SQS(20) are the following:

$$\begin{array}{ll}
\{1_0, 2_0, 3_1, 2_3\}, & \{1_0, 4_0, 1_1, 2_3\},\\
\{1_0, 2_0, 4_1, 4_3\}, & \{1_0, 0_0, 0_1, 2_3\},\\
\{1_0, 3_0, 2_1, 2_3\}, & \{1_0, 2_0, 3_0, 2_2\},\\
\{1_0, 2_0, 0_1, 1_3\}, & \{1_0, 2_0, 4_0, 4_2\},\\
\{1_0, 3_0, 0_1, 3_3\}, & \{1_0, 2_0, 3_2, 0_2\},\\
\{0_0, 1_0, 1_1, 4_3\}, & \{4_0, 1_1, 3_3, 0_2\},\\
\{1_0, 3_0, 1_1, 0_3\}, & \{0_1, 0_2, 0_3, 0_4\},\\
\{1_0, 3_0, 4_1, 1_3\}. &
\end{array}$$

The cyclic permutation $x_i \to (x+1)_{(i+1)}$ with $x+1$ reduced mod 5 and with $i+1$ reduced mod 4 applied to these blocks will give us our cyclic SQS(20). To see that it is not S-cyclic we present an isomorphic copy with $Q = \{0, 1, 2, \ldots, 19\}$:

Base block	Difference quadruple	Base block	Difference quadruple
{0, 5, 6, 9}	(5, 1, 3, 11)	{0, 1, 6, 13}	(1, 5, 7, 7)
{0, 3, 7, 10}	(3, 4, 3, 10)	{0, 2, 3, 9}	(2, 1, 6, 11)
{0, 1, 9, 10}	(1, 8, 1, 10)	{0, 4, 9, 11}	(4, 5, 2, 9)
{0, 1, 3, 8}	(1, 2, 5, 12)	{0, 4, 8, 14}	(4, 4, 6, 6)
{0, 1, 5, 14}	(1, 4, 9, 6)	{0, 2, 4, 12}	(2, 2, 8, 8)
{0, 2, 5, 13}	(2, 3, 8, 7)	{0, 2, 6, 8}	(2, 4, 2, 12)
{0, 3, 4, 5}	(3, 1, 1, 15)	{0, 5, 10, 15}	(5, 5, 5, 5)
{0, 3, 6, 15}	(3, 3, 9, 5)		

The cyclic permutation $i \to i+1$ (mod 20) applied to the base blocks above will give us a cyclic SQS(20), isomorphic to the one previously given. Clearly, there are difference quadruples that are not symmetric.

4. Concluding remarks. Although we have shown that the spectrum of cyclic 3-quasigroup satisfying the conditions mentioned in Section 2 is not vacuous, it is not clear that it is non-trivial. The first problem then would be to find examples of these 3-quasigroups for small orders, say 11, 13 or 17 (**P 1172**). The second would be to find an infinite class (**P 1173**).

REFERENCES

[1] J. Doyen and M. Vandensavel, *Non-isomorphic Steiner quadruple systems*, Bulletin de la Société Mathématique de Belgique 23 (1971), p. 393-410.

[2] H. Hanani, *On quadruple systems*, Canadian Journal of Mathematics 12 (1960), p. 145-147.

[3] R. K. Jain, *On cyclic Steiner quadruple systems*, Thesis, McMaster University, Hamilton 1971.

[4] C. C. Lindner and A. Rosa, *Steiner quadruple systems — a survey*, Discrete Mathematics 21 (1978), p. 147-181.

[5] K. T. Phelps, *A construction of disjoint Steiner quadruple systems*, Proceedings 8th S. E. Conference on Combinatorics, Graph Theory and Computing, Utilitas Math. Publishing, p. 559-568.

Reçu par la Rédaction le 25. 10. 1977