This is a preprint of an article accepted for publication in Ars Combinatoria, **9**, 1980, 51–58.

ON THE STRUCTURE OF S-CYCLIC STEINER QUADRUPLE SYSTEMS

M.J.Grannell and T.S.Griggs

1980

1 Introduction

A Steiner quadruple system of order v, denoted by SQS(v), consists of a pair (A, B) where A is a v-element set and B is a family of four-element subsets of A (called blocks) with the property that each three-element subset of A lies in precisely one block. Such a system is said to be cyclic if B is invariant under a cyclic group of order v.

Any cyclic SQS(v) will be isomorphic to a system in which $A = V$ (the set of residue classes modulo v) and where B is invariant under the cyclic group $C_v = \langle i \rightarrow> i + 1 \pmod{v}\rangle$. Any system of this type will be composed of orbits generated by the action of C_v on four-element subsets of V. An orbit generated in this way is said to be symmetric if it is invariant under the mapping $i \rightarrow -i \pmod{v}$.

An SQS(v) is said to be S-cyclic if it is isomorphic to a cyclic system, of the form described above, each of whose orbits is symmetric. (This is an alternative, but equivalent, definition to that usually given e.g. in [6]).

In [6] Lindner and Rosa partition the admissible orders for SQS(v) into four classes:

A. $v \equiv 2$ or $10 \pmod{24}$,

B. $v \equiv 4$ or $20 \pmod{24}$,

C. $v \equiv 14$ or $22 \pmod{24}$,

D. $v \equiv 8$ or $16 \pmod{24}$.

Cyclic systems in classes B and D necessarily contain the unique $\frac{1}{4}$-orbit (i.e. the orbit with $v/4$ blocks), while those in C and D contain an odd number of $\frac{1}{2}$-orbits (i.e. orbits with $v/2$ blocks). At the time [6] was written, all known cyclic SQS(v) were S-cyclic and, with the single exception of the unique S-cyclic SQS(20) constructed by Jain [5], all lay in class A. Subsequently several cyclic (but non S-cyclic) systems have been discovered (c.f. [7], [1], [4]).

In [8], Phelps gives a complete enumeration of cyclic SQS(20). He also notes that there are no S-cyclic systems in classes C and D (in fact no S-cyclic system may contain a $\frac{1}{2}$-orbit). He then poses the question of whether S-cyclic systems necessarily exist whenever v lies in classes A or B. Diener [2] shows that this is not the case by proving that if $v \equiv 0 \pmod 7$ then there does not exist an S-cyclic SQS(v).

In this paper we establish an improved necessary condition on v for the existence of an S-cyclic SQS(v), thereby showing that for many values of v in classes A and B (including those covered by Diener's result), S-cyclic SQS(v) do not exist. In the course of establishing the condition we also prove a general result (Theorem 2(ii)) concerning the structure of S-cyclic systems and in Theorem 4 we establish a further result of this type. These results facilitate the construction of an S-cyclic SQS(v) for $v = 52$: this was the smallest value of v, satisfying the improved necessary condition, for which an S-cyclic system was not previously known. (Recently C.J.Cho has also constructed S-cyclic SQS(v) for $v = 52, 68$ and 122).

2 General Results

THEOREM 1.
Suppose $\mathcal{O}$ is an orbit of blocks, with elements drawn from the residue classes modulo uv, under the action of the cyclic group $C_{uv} = \langle i \to i+1 \pmod{uv}\rangle$. Suppose also that $\mathcal{O}$ is invariant under the mapping $i \to -i \pmod{uv}$ and that v is even. Then if $\mathcal{O}$ contains a block of the form $\{ua, ub, uc, x\}$, x is necessarily of the form ud for some $d \in \{0, 1, \ldots, (v-1)\}$.

Proof.
If $\mathcal{O}$ contains a block of the form $\{ua, ub, uc, x\}$ then it will contain just four (not necessarily distinct) blocks each containing 0. These will be of the form $\{0, u\alpha, u\beta, z\}$, $\{-u\alpha, 0, u(\beta-\alpha), z-u\alpha\}$, $\{-u\beta, u(\alpha-\beta), 0, z-u\beta\}$, $\{-z, u\alpha - z, u\beta - z, 0\}$, where $\alpha = b - a$, $\beta = c - a$ and $z = x - ua$ (all arithmetic being modulo uv).

Since $\mathcal{O}$ is invariant under $i \to -i \pmod{uv}$, the block $\{0, -u\alpha, -u\beta, -z\}$ must be one of the four blocks listed above. We show that each possibility leads to the conclusion $z = u\gamma$ for some $\gamma \in \{0, 1, \ldots, (v-1)\}$, and hence $x = ud$ for some $d \in \{0, 1, \ldots, (v-1)\}$.

(i) Suppose $\{0, -u\alpha, -u\beta, -z\} = \{0, u\alpha, u\beta, z\}$. If $z = 0, -u\alpha$ or $-u\beta$ there is nothing to prove. Otherwise $z = -z$ and so either $z = 0$ or

$z = (uv)/2$. In the latter case, since v is even, we may write $z = u(v/2)$.

(ii) Suppose $\{0, -u\alpha, -u\beta, -z\} = \{-u\alpha, 0, u(\beta - \alpha), z - u\alpha\}$. As before, there is nothing to prove unless $-z = z - u\alpha$. But in this case we must also have $-u\beta = u(\beta - \alpha)$. Hence $-ua = -2u\beta$, and so $-z = z - 2u\beta$. This gives $2z = 2u\beta$ and it follows that either $z = u\beta$ or $z = u\beta + (uv)/2$. In the latter case we may again write $z = u(\beta + v/2)$.

(iii) The case $\{0, -u\alpha, -u\beta, -z\} = \{-u\beta, u(\alpha - \beta), 0, z - u\beta\}$ can be dealt with similarly to (ii).

(iv) Suppose $\{0, -u\alpha, -u\beta, -z\} = \{-z, u\alpha - z, u\beta - z, 0\}$. Then either $-u\alpha = u\alpha - z$ or $-u\beta = u\alpha - z$ and there is nothing to prove.

THEOREM 2.
Suppose that v is even, $v > 2$, and that an S-cyclic SQS(uv) exists. Then

(i) there exists an S-cyclic SQS(v),

(ii) given any S-cyclic SQS(v), S_v, there is an S-cyclic SQS(uv) containing an isomorphic image of S_v; in the usual representation such an embedding is given by $i \to ui \quad (i \in \{0, 1, \ldots, (v-1)\})$.

Proof.

(i) Let S_{uv} be an S-cyclic SQS(uv) represented in the usual way on the residue classes modulo uv.

Choose any three distinct elements from $\{0, u, 2u, \ldots, (v-1)u\}$, ua, ub, uc, say (this is possible since $v > 2$). S_{uv} necessarily contains a block of the form $\{ua, ub, uc, x\}$. By Theorem 1, x must be of the form ud for some d, and clearly $d \neq a, b$ or c. Hence those blocks in S_{uv} which have a common factor u will form an SQS(v), S_v say, on the points $\{0, u, 2u, \ldots, (v-1)u\}$. Each orbit $\mathcal{O}$ in S_{uv} containing such a block will give rise to an orbit $\mathcal{O}'$ in S_v, formed from the blocks of this type under the action of the group $\langle i \to i + u \pmod{uv}\rangle$; since $\mathcal{O}$ is invariant under $i \to -i \pmod{uv}$, so also will be $\mathcal{O}'$: Hence S_v is S-cyclic.

(ii) Suppose that S_{uv} is an S-cyclic SQS(uv) (represented in the usual way) and that S_v^* is any S-cyclic SQS(v). We may assume that the latter system is based on the points $\{0, u, 2u, \ldots, (v-1)u\}$, that it has an automorphism group $\langle i \to i+u \pmod{uv}\rangle$, and that the orbits forming it are invariant under $i \to -i \pmod{uv}$.

Let R_{uv} denote the design formed from S_{uv} by deleting those orbits contributing blocks to the SQS(v) sub-system, S_v, described in part (i). To R_{uv} we add all orbits formed from the blocks of S_v^* under the action of the group $\langle i \to i+1 \pmod{uv}\rangle$; the resulting design we refer to as S_{uv}^*.

Since S_v and S_v^*, contain exactly the same three-element subsets of $\{0, u, 2u, \ldots, (v-1)u\}$, the orbits removed from S_{uv} to form R_{uv} and the orbits added to R_{uv} to form S_{uv}^* will contain exactly the same three-element subsets of $\{0, 1, \ldots, vu-1\}$. Hence S_{uv}^* is an SQS(uv).

To complete the proof note that R_{uv} is composed of symmetric cyclic orbits and that the orbits from the blocks of S_v^* are also symmetric and cyclic. It follows that S_{uv}^* is S-cyclic. Factoring out the u from the blocks of S_v^* gives an isomorphic S-cyclic SQS(v) represented in the usual way; clearly S_{uv}^* contains a copy of this system under the mapping $i \to ui \quad (i \in \{0, 1, \ldots, (v-1)\})$.

THEOREM 3.
A necessary condition for the existence of an S-cyclic SQS(v) is that $v = 2n$ or $4n$, where the prime factors of n are all of the forms $12s+1$ or $12s+5$ $(s = 0, 1, 2, \ldots)$.
Proof.
Suppose that an S-cyclic SQS(v) exists. The admissibility condition shows that $v \equiv 2$ or $4 \pmod 6$. Hence v is even and, since v cannot lie in Class D, v is not divisible by 8. Therefore, v is of the form $2n$ or $4n$ where n is odd. Clearly n cannot be divisible by 3 and so n must be a product of prime factors each of which has one of the following forms: $12s+1, 12s+5, 12s+7, 12s+11$.

Suppose that n had a factor $12s+7$. Then we could write $v = uv'$ where $v' = 24s+14$. By Theorem 2(i), the existence of an S-cyclic SQS(v) implies that of an S-cyclic SQS(v'). However, v' lies in class C and so there cannot be an S-cyclic SQS(v'). Hence n cannot have a factor $12s+7$. Similarly we may prove that n cannot have a factor $12s+11$.

Through the remainder of this section we shall assume that v satisfies the admissibility condition, $v \equiv 2$ or $4 \pmod 6$. We shall be solely concerned with orbits formed from three-element subsets and four-element subsets of the set of residue classes modulo v, under the action of C_v. We make the following definitions, (see also [8]).

DEFINITIONS.
An orbit $\mathcal{O}$ of four-element subsets (i.e. blocks) is said to be suitable if for every pair of distinct blocks $S, T \in \mathcal{O}$, we have $|S \cap T| < 3$.

Two distinct orbits $\mathcal{O}_1$ and $\mathcal{O}_2$, of blocks are said to be compatible if for every pair of blocks, S, T with $S \in \mathcal{O}_1$ and $T \in \mathcal{O}_2$, we have $|S \cap T| < 3$. Any cyclic SQS(v) will consist of a union of suitable and pairwise compatible orbits.

Any block contains four three-element subsets. Since $v \neq 0 \pmod 3$, any orbit of three-element subsets is necessarily full (i.e. it contains v distinct three-element subsets). Therefore any suitable and full orbit, $\mathcal{O}$, (of blocks) will give rise to precisely four distinct full orbits of three-element subsets. We shall refer to these as the suborbits of $\mathcal{O}$. If $\mathcal{O}_1$ and $\mathcal{O}_2$ are incompatible orbits (of blocks) then $\mathcal{O}_1$ and $\mathcal{O}_2$ must have at least one suborbit in common.

THEOREM 4. Suppose that S is an S-cyclic SQS(v) and that $\mathcal{O}$ is a symmetric suitable full orbit (SSFO) not contained in S. Then there exist precisely two distinct full orbits $\mathcal{O}_1, \mathcal{O}_2$, contained in S which are incompatible with $\mathcal{O}$.

Proof.
We may assume S has its usual representation. We note firstly that if $\mathcal{O}'$ and $\mathcal{O}''$ are both SSFO's and both contain the same suborbits then $\mathcal{O}' = \mathcal{O}''$. For a proof of this see [8, lemma 2.3].

Next we consider the action of the mapping $i \to -i \pmod v$ on orbits of three-element subsets. If A is such an orbit we shall denote by $-A$ the orbit which is its image under this mapping. For certain orbits we shall have $A = -A$; namely those containing blocks of the form $\{0, x, -x\}$. If $x \neq \pm\frac{v}{4}$ it is easily seen that such an orbit occurs as a suborbit of one and only one SSFO, namely that generated by $\{0, x, -x, v/2\}$; any such SSFO is therefore necessarily included in S (see [3]). For $x = \pm\frac{v}{4}$ the resulting orbit of four-element subsets is the $\frac{1}{4}$-orbit, and is again included in S

Suppose now that $\mathcal{O}$ is an SSFO not in S. Then $\mathcal{O}$ must contain four distinct suborbits $A, -A, B, -B$. There is an orbit $\mathcal{O}_1$ in S containing A and hence also $-A$. Likewise, there is an orbit $\mathcal{O}_2$ in S containing B and hence also $-B$. Neither $\mathcal{O}_1$ nor $\mathcal{O}_2$ can be the $\frac{1}{4}$-orbit and so both are SSFO's. If $\mathcal{O}_1$ and $\mathcal{O}_2$ were identical then both $\mathcal{O}$ an $\mathcal{O}_1$ would contain the same suborbits and we should have $\mathcal{O} = \mathcal{O}_1$, which is not the case. Hence $\mathcal{O}_1 \neq \mathcal{O}_2$. Clearly, there can be no other orbits in S which are incompatible with $\mathcal{O}$.
The proof is therefore complete.

Before dealing with the case $v = 52$ we make some general observations. Suppose that an S-cyclic SQS(v) exists.Put

$$
\begin{aligned}
S(v) &= \text{the total number of SSFOs,}\\
N(v) &= \text{the number of SSFOs contained in the SQS}(v),\\
s_i(v) &= \text{the total number of SSFOs which are incompatible with}\\
&\qquad \text{precisely } i \text{ other SSFOs,}\\
n_i(v) &= \text{the number of SSFOs contained in the SQS}(v)\text{which are}\\
&\qquad \text{incompatible with precisely } i \text{ other SSFOs.}
\end{aligned}
$$

Clearly $\sum n_i(v) = N(v)$ and $n_i(v) \leq s_i(v)$. Theorem 4 also ensures that $\sum in_i(v) = 2(S(v) - N(v))$ and that $n_0(v) = s_0(v)$ and $n_1(v) = s_1(v)$.

3 The case $v = 52$

Computer calculation gives $S(52) = 288$ and, since no S-cyclic system can contain a $\frac{1}{2}$-orbit, $N(52) = 106$. Likewise we obtain $S(26) = 60$ and $N(26) = 25$.

Computer listings of compatibility for $v = 52$ and 26 give the following values for the $s_i(v)$ s.

(a) $v = 52$: $s_0(52) = 0$, $s_1(52) = 12$, $s_2(52) = 8$, $s_3(52) = 54$, $s_4(52) = 219$.

(b) $v = 26$: $s_0(26) = 0$, $s_1(26) = 6$, $s_2(26) = 3$, $s_3(26) = 24$, $s_4(26) = 27$.

Consider now the collection $\mathcal{E}$ of all those SSFOs under C_{52} which contain blocks of the form $\{2a, 2b, 2c, 2d\}$. Orbits of this type correspond (under the mapping $i \to 2i$) to the 60 SSFOs generated by C_{26}. Hence $|\mathcal{E}| = S(26) = 60$. Denote by $\mathcal{F}$ the remaining SSFOs generated by C_{52} and put $S^* = |\mathcal{F}|$. We have $S^* = S(52) - S(26) = 228$. Note that by Theorem 1, if $\mathcal{O}_1$ and $\mathcal{O}_2$ are SSFOs in $\mathcal{E}$ and $\mathcal{F}$ respectively then $\mathcal{O}_1$ and $\mathcal{O}_2$ must be compatible.

Define s_i^* to be the total number of SSFOs contained in $\mathcal{F}$ which are incompatible with precisely i other SSFOs. Then we must have $s_i^* = s_i(52) - s_i(26)$ for each i. This gives

$$s_0^* = 0, \quad s_1^* = 6, \quad s_2^* = 0, \quad s_3^* = 30, \quad s_4^* = 192.$$

Suppose now that an S-cyclic SQS(52) exists. For this particular system define

$$\begin{aligned} n_i^* = {} & \text{the number: of SSFOs contained in } \mathcal{F} \text{ which are} \\ & \text{also contained in the SQS(52) and which are} \\ & \text{incompatible with precisely } i \text{ other SSFOs, and} \\ N^* = {} & \text{the number of SSFOs contained in } \mathcal{F} \text{ which} \\ & \text{are also contained in the SQS(52).} \end{aligned}$$

We have immediately that $\sum n_i^* = N^* = N(52) - N(26) = 81$. From Theorem 4 we can deduce that $\sum i n_i^* = 2(S^* - N^*) = 294$, and also that $n_0^* = s_0^* = 0$, $n_1^* = s_1^* = 6$. Finally, since $s_2^* = 0$, we have $n_2^* = 0$. Solving the equations for n_3^* and n_4^* gives $n_3^* = 12$ and $n_4^* = 63$.

Reference to computer listings shows that of the 30 orbits contributing to s_3^*, 6 are incompatible with those contributing to s_1^*. The remaining 24 partition into 12 pairs; the two orbits in each pair being incompatible.

From this point onwards it appears necessary to employ heuristic argument. However, even here Theorem 4 is of considerable use in narrowing the choice.

We list below the unique $\frac{1}{4}$-orbit and 81 mutually compatible orbits from the collection $\mathcal{F}$. Together with the orbits in $\mathcal{E}$ generated from any S-cyclic SQS(26), these form an S-cyclic SQS(52). To give a specific example, we may complete the system by including the particular SQS(26) given in [6]; the list below includes the 25 orbits for this system.

TABULATION.
Generators for symmetric cyclic orbits forming an S-cyclic SQS(52).

(a) 1/4-orbit. $\{0,13,26,39\}$.

(b) 81 orbits in $\mathcal{F}$. $\{0,1,2,27\}$, $\{0,1,3,4\}$, $\{0,1,5,6\}$,
$\{0,1,7,8\}$, $\{0,1,9,44\}$, $\{0,1,10,11\}$, $\{0,1,12,13\}$, $\{0,1,14,39\}$,
$\{0,1,15,16\}$, $\{0,1,17,18\}$, $\{0,1,19,34\}$, $\{0,1,20,33\}$, $\{0,1,21,22\}$,
$\{0,1,23,30\}$, $\{0,1,24,25\}$, $\{0,2,5,7\}$, $\{0,2,9,45\}$, $\{0,2,11,13\}$,
$\{0,2,15,39\}$, $\{0,2,17,37\}$, $\{0,2,19,35\}$, $\{0,2,21,23\}$, $\{0,2,25,29\}$,
$\{0,3,6,29\}$, $\{0,3,7,10\}$, $\{0,3,8,11\}$, $\{0,3,9,12\}$, $\{0,3,13,42\}$,
$\{0,3,14,41\}$, $\{0,3,15,18\}$, $\{0,3,16,19\}$, $\{0,3,17,38\}$, $\{0,3,20,23\}$,
$\{0,3,21,34\}$, $\{0,3,22,25\}$, $\{0,3,24,27\}$, $\{0,4,9,13\}$, $\{0,4,11,15\}$,
$\{0,4,17,39\}$, $\{0,4,19,23\}$, $\{0,4,21,25\}$, $\{0,5,10,31\}$, $\{0,5,11,46\}$,
$\{0,5,12,45\}$, $\{0,5,13,18\}$, $\{0,5,14,43\}$, $\{0,5,15,20\}$, $\{0,5,16,41\}$,
$\{0,5,17,22\}$, $\{0,5,19,24\}$, $\{0,5,21,36\}$, $\{0,5,23,28\}$, $\{0,5,25,30\}$,
$\{0,6,13,19\}$, $\{0,6,15,21\}$, $\{0,6,23,35\}$, $\{0,6,25,31\}$, $\{0,7,14,33\}$,
$\{0,7,15,22\}$, $\{0,7,17,24\}$, $\{0,7,18,25\}$, $\{0,7,20,27\}$, $\{0,7,21,28\}$,
$\{0,7,23,36\}$, $\{0,8,19,41\}$, $\{0,8,21,29\}$, $\{0,8,23,37\}$, $\{0,8,25,33\}$,
$\{0,9,18,35\}$, $\{0,9,19,42\}$, $\{0,9,20,29\}$, $\{0,9,21,40\}$, $\{0,9,22,31\}$,
$\{0,9,24,33\}$, $\{0,9,25,34\}$, $\{0,10,21,41\}$, $\{0,10,25,35\}$, $\{0,11,22,37\}$,
$\{0,11,23,34\}$, $\{0,11,24,35\}$, $\{0,12,25,37\}$.

(c) 25 orbits in $\mathcal{E}$. $\{0,2,4,28\}$, $\{0,2,6,8\}$, $\{0,2,10,12\}$,
$\{0,2,14,16\}$, $\{0,2,18,20\}$, $\{0,2,22,24\}$, $\{0,4,8,30\}$, $\{0,4,10,46\}$,
$\{0,4,12,44\}$, $\{0,4,14,42\}$, $\{0,4,16,20\}$, $\{0,4,18,38\}$, $\{0,4,22,34\}$,
$\{0,4,24,32\}$, $\{0,6,12,32\}$, $\{0,6,14,20\}$, $\{0,6,18,24\}$, $\{0,6,22,28\}$,
$\{0,8,16,34\}$, $\{0,8,18,42\}$, $\{0,8,22,38\}$, $\{0,8,24,36\}$, $\{0,10,20,36\}$,
$\{0,10,22,32\}$, $\{0,12,24,38\}$.

In conclusion we should like to express our gratitude to the computer operations staff at Preston Polytechnic for their patient co-operation. We should also like to thank the referee for his helpful comments and suggestions.

References

[1] C. J. Cho, *A construction for cyclic quadruple systems*, M.Sc.thesis, McMaster University, Hamilton, Ontario (1979).

[2] I. Diener, *S-Zyklische Steinersysteme*, Diplomarbeit, Institut für Numerische und Angewandte Mathematik, Universitat Gottingen (1979).

[3] F. Fitting, *Zyklische Lösungen des Steiner'schen Problems*, Nieuw Arch. Wisk. 11 (2) (1915), 140–148.

[4] M. J. Grannell and T. S. Griggs, *A non-symmetric cyclic Steiner quadruple system*, Preston Polytechnic Research Note (1978).

[5] R. K. Jain, *On cyclic Steiner quadruple systems*, M.Sc. thesis, McMaster University, Hamilton, Ontario (1971).

[6] C. C. Lindner and A. Rosa, *Steiner quadruple systems - a survey*, Discrete Math. 21 (1978),147–181.

[7] K. T. Phelps, *A note on the construction of cyclic quadruple systems*, Colloq. Math. (to appear).

[8] K. T. Phelps, *On cyclic Steiner systems* $S(3, 4, 20)$, (to appear).

Division of Mathematics,
Preston Polytechnic,
Corporation Street,
PRESTON,
Lancs. PR1 2TQ,
England.