S-CYCLIC STEINER SYSTEMS

M. J. Grannell and T. S. Griggs
Division of Mathematics
Preston Polytechnic
Corporation Street
Preston PR1 2TQ
England.

1983

1 Introduction.

In his paper [5], Immo Diener shows that for given t and k the number of values of v for which an S-cyclic Steiner system $\mathrm{S}(t,k,v)$ exists is finite except possibly for $t=3$ and k even. In this paper we show that for non-trivial systems "finite" may be replaced by "zero" except in the case $t=3$, and indeed in the case $t=3$ and k odd "finite" may be replaced by "at most one", this value of v being equal to k^2-2k+2.

A Steiner system $\mathrm{S}(t,k,v)$ is an ordered pair $(V,\mathcal{B})$ where V is a set of cardinality v and $\mathcal{B}$ is a collection of k-element subsets of V which has the property that each t-element subset of V is contained in precisely one member of $\mathcal{B}$. The members of $\mathcal{B}$ are referred to as blocks or k-blocks and the t-element subsets of V as subblocks or t-blocks. The Steiner system $\mathrm{S}(t,k,v)$ is said to be cyclic if it has an automorphism of order v. Any such system S will be isomorphic to one T in which V is the set of residue classes modulo v and the automorphism is $z\to z+1 \pmod v$. We will say that T is a standard representation of S and that T is in standard form.

Suppose T is a cyclic $\mathrm{S}(t,k,v)$ in standard form and that $B=\{x_1,x_2,\ldots, x_k\}$ is a block of T. Then $B+i=\{x_1+i,x_2+i,\ldots,x_k+i\}$ is also a block of T for each $i=1,2,\ldots,v-1$, the arithmetic being performed mod v. The collection of blocks $\{B+i,\ i=0,1,\ldots,v-1\}$ is called an orbit. If the cardinality of the orbit is v it will be called a full orbit, otherwise it will be referred to as a small orbit. Any orbit is uniquely characterised by its difference set $\langle d_1, d_2, \ldots, d_k\rangle$ which is a cyclically ordered k-tuple obtained from any block $\{x_1, x_2, \ldots, x_k\}$ of the orbit (ordered so that $0 \le x_1 < x_2 < \ldots < x_k < v$) by taking $d_i = x_i - x_{i-1}$ for $i = 2, 3, \ldots, k$ and $d_1 = x_1 + v - x_k$.

Suppose now that $B = \{x_1, x_2, \ldots, x_k\}$ is a k-element subset of the set of residue classes modulo v. We denote by $-B$ the set obtained by applying the mapping $z \to v - z \pmod v$ to the elements of B. If S is a cyclic $\mathrm{S}(t, k, v)$ we say that S is R-cyclic if there is a standard representation T of S such that for each block B of T, $-B$ is also a block of T. If, in addition the block $-B$ always lies in the same orbit as B then we say that S is S-cyclic. The notion of an S-cyclic system was first introduced in connection with Steiner quadruple systems. Interest stems from the substantial reduction in computation required to construct such systems as opposed to general cyclic systems (see, for example, [5], [6], [7], [8], [10]). Following the proof of the main theorem we illustrate the computational process by giving a construction of $\mathrm{S}(3, 5, 17)$.

2 General Result

THEOREM. Suppose that $1 < t < k < v$. Then an S-cyclic $\mathrm{S}(t, k, v)$ can only exist if $t = 3$. Moreover if $t = 3$ and k is odd, then an S-cyclic $\mathrm{S}(t, k, v)$ can only exist if $v = k^2 - 2k + 2$.

Remark: The class of S-cyclic $\mathrm{S}(3, k, k^2 - 2k + 2)$ with k odd is non-empty as the construction of $\mathrm{S}(3, 5, 17)$ given in Section 3 demonstrates. However there is no $\mathrm{S}(3, 7, 37)$ as is well known. The existence of further S-cyclic systems with these parameters appears to be an open question.

Proof: The proof breaks into eight cases corresponding to the parity of t, k and v. In the course of the proof, the ordered parameter set (t, k, v) will be called admissible if $\binom{k-i}{t-i} | \binom{v-i}{t-i}$ for $i = 0, 1, \ldots, t-1$; this condition being necessary for the existence of an $\mathrm{S}(t, k, v)$. In particular, taking $i = t - 1$, the existence of an $\mathrm{S}(t, k, v)$ implies that $(k - t + 1)|(v - t + 1)$.

We only consider non-trivial systems where $1 < t < k < v$. For such systems an elementary argument (see [1]) gives the inequality $v - t + 1 \ge (k - t + 2)(k - t + 1)$, which we refer to as (I). As was observed in [5], R-cyclic (and therefore S-cyclic) $\mathrm{S}(2, k, v)$ do not exist; hence we may assume below that $t \ge 3$. Further in [5] Diener proves that if k is odd then an S-cyclic k-block orbit will have a difference set of the form $\langle d_1, d_2, \ldots, d_m, d_{m+1}, d_m, \ldots, d_2, d_1\rangle$ where $k = 2m + 1$, while if k is even then the difference set is either of the form $\langle d_1, d_2, \ldots, d_m, d_m, \ldots, d_2, d_1\rangle$ or of the form $\langle d_1, d_2, \ldots, d_{m-1}, e, d_{m-1}, \ldots, d_2, d_1, f\rangle$ where $k = 2m$.

The eight cases of our proof may be arranged in order of increasing complexity as follows:

(i) t even, k odd, v even,

(ii) t odd, k even, v odd,

(iii) t even, k odd, v odd,

(iv) t odd, k odd, v odd,

(v) t odd, k odd, v even,

(vi) t even, k even, v odd,

(vii) t even, k even, v even,

(viii) t odd, k even, v even $(t > 3)$.

Cases (i) and (ii). Here the parameter sets are inadmissible since $(k - t + 1)$ does not divide $(v - t + 1)$.

Case (iii). Suppose that an R-cyclic $\mathrm{S}(t, k.v)$ exists, then it must contain a k-block of the form

$$\{1, 2, \ldots, u, \alpha_1, \ldots, \alpha_{k-t}, v - u, \ldots, v - 2, v - 1\}$$

where $u = t/2$, and where the α_i s (of which there is an odd number) are all distinct and satisfy $u < \alpha_i < v - u$ or $\alpha_i = 0$ for each $i = 1, 2, \ldots, k - t$. Consideration of the mapping $z \to v - z \pmod{v}$ reveals that one of the α_i s must equal 0. But then the mapping $z \to z + 1 \pmod{v}$ applied to the above k-block gives a different k-block in the same orbit with a t-block intersection. It follows that in Case (iii) no R-cyclic $\mathrm{S}(t, k, v)$ can exist and so, therefore, no S-cyclic $\mathrm{S}(t, k, v)$ can exist.

Case (iv). Put $u = (t - 1)/2$ and $m = (k - 1)/2$. We define a symmetric t-block to be a t-block of the form $\{0, \alpha_1, \ldots, \alpha_u, v - \alpha_u, \ldots, v - \alpha_1\}$ with $1 \le \alpha_1 < \alpha_2 < \ldots < \alpha_u \le (v - 1)/2$. Clearly there $\binom{(v-1)/2}{u}$ symmetric t-blocks. Each S-cyclic k-block orbit has a difference set of the form $\langle d_1, d_2, \ldots, d_m, d_{m+1}, d_m, \ldots, d_2, d_1\rangle$ and so contains a k-block $\{0, x_1, \ldots, x_m, v - x_m, \ldots, v - x_1\}$ with $0 < x_1 < x_2 < \ldots < x_m < v/2$. Hence each S-cyclic k-block orbit gives rise to at least $\binom{m}{u}$ distinct symmetric t-blocks. If an S-cyclic $\mathrm{S}(t, k, v)$ does exist, composed of N k-block orbits, then it follows that $\binom{(v-1)/2}{u}/\binom{m}{u} \geq N$. However, an $\mathrm{S}(t,k,v)$ contains $\binom{v}{t}/\binom{k}{t}$ k-blocks and so $N \geq \binom{v}{t}/\left(v\binom{k}{t}\right)$. It follows that

$$\binom{(v-1)/2}{u}\bigg/\binom{m}{u} \geq \binom{v}{t}\bigg/\left(v\binom{k}{t}\right)$$

which reduces to $k(k-2)\ldots(k-t+1) \geq (v-2)(v-4)\ldots(v-t+1)$, which we call (J).

When t $= 3$ this gives $k(k-2) \geq v-2$, and so $v \leq k^2-2k+2$. But (I) gives $v-2 \geq (k-1)(k-2)$. Hence $k^2-3k+4 \leq v \leq k^2-2k+2$. Note that $(k-2)|(v-2)$, so that the only possible values of v for $t=3$ are $v=k^2-3k+4$ and $v=k^2-2k+2$. The existence of $\mathrm{S}(3,k,k^2-3k+4)$ implies, through the admissibility condition, that $k|(k^2-3k+3)(k^2-3k+4)$ and so $k|12$ which is not possible. This leaves $\mathrm{S}(3,k,k^2-2k+2)$ as an outstanding possibility.

Now suppose $t \geq 5$. Put $d=k-t$, so that (I) gives $v-t+1 \geq d^2+3d+2$, and hence $v-t+3 \geq d^2+3d+4$. Noting $v-2 \geq k$, $v-4 \geq k-2$, etc. we deduce from (J) that $(d+5)(d+3)(d+1) \geq (d^2+3d+4)(d^2+3d+2)$ but this is plainly false when $d \geq 2$.

Case (v). The argument follows closely that of the previous case. The number of symmetric t-blocks is now $\binom{(v-2)/2}{u}$ and in place of (J) we obtain $k(k-2)\ldots(k-t+1) \geq (v-1)(v-3)\ldots(v-t+2)$, which we call (K).

When $t=3$ this gives $k(k-2) \geq v-1$, and so $v \leq k^2-2k+1$. Using (I) we deduce that $k^2-3k+4 \leq v \leq k^2-2k+1$ and a similar argument to that of Case (iv) disposes of $t=3$.

Now suppose $t \geq 5$. With $d=k-t$, using (I) and noting $v-1 \geq k$, $v-3 \geq k-2$, etc. we deduce from (J) that $(d+5)(d+3)(d+1) \geq (d^2+3d+5)(d^2+3d+3)$. But again this is false for $d \geq 2$.

Case (vi). Put $u=t/2$ and $m=k/2$. Since v is odd an S-cyclic k-block orbit cannot have a difference set of the form $\langle d_1,d_2,\ldots,d_m,d_m,\ldots,d_2,d_1\rangle$. Consequently all S-cyclic k-block orbits have a difference set of the form $\langle d_1,d_2,\ldots,d_{m-1},e,\ d_{m-1},\ldots,d_2,d_1,f\rangle$ where precisely one of e and f is even; without loss of generality we can assume that it is e. It follows that any S-cyclic k-block orbit contains a block of the form

$$\{0,x_1,\ldots,x_{m-1},x_{m-1}+e,2x_{m-1}+e-x_{m-2},\ldots,2x_{m-1}+e-x_1,2x_{m-1}+e\}$$

and putting $g=2x_{m-1}+e$, so that g is even, this is of the form

$$\{0,x_1,\ldots,x_{m-1},g-x_{m-1},g-x_{m-2},\ldots,g-x_1,g\},$$

(with elements in ascending order). With $h=g/2$, the mapping $z \to z-h$ (mod v) transforms this block to

$$\{v-h,v-h+x_1,\ldots,v-h+x_{m-1},h-x_{m-1},\ldots,h-x_1,h\}$$

which may be re-arranged with elements in ascending order into the form

$$\{y_1, y_2, \ldots, y_m, v-y_m, \ldots, v-y_2, v-y_1\}$$

with $1 \leq y_1 < y_2 < \ldots < y_m \leq (v-1)/2$. Every S-cyclic k-block orbit contains such a block.

We define a symmetric t-block to be one of the form

$$\{\alpha_1, \alpha_2, \ldots, \alpha_u, v-\alpha_u, \ldots, v-\alpha_2, v-\alpha_1\}$$

where $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_u \leq (v-1)/2$.

Clearly there are $\binom{(v-1)/2}{u}$ symmetric t-blocks. Each S-cyclic k-block orbit contains a block of the type described in the previous paragraph and so gives rise to at least $\binom{m}{u}$ symmetric t-blocks. As in Case (iv) it follows that

$$\binom{(v-1)/2}{u} \Big/ \binom{m}{u} \geq \binom{v}{t} \Big/ \left(v\binom{k}{t}\right)$$

which now reduces to $(k-1)(k-3)\ldots(k-t+1) \geq (v-2)(v-4)\ldots(v-t+2)$ which we call (L).

When $t=4$ this gives $(k-1)(k-3) \geq v-2$ and so $v \leq k^2-4k+5$. But (I) gives $v-3 \geq (k-2)(k-3)$. Hence $k^2-5k+9 \leq v \leq k^2-4k+5$. Note also that $(k-3)|(v-3)$, so that the only possible value of v for $t=4$ is $v = k^2-5k+9$. This, in turn, is impossible since the admissibility condition gives $(k-1)|(k^2-5k+8)(k^2-5k+7)$ and so $(k-1)|12$ which has no solutions for k even and greater than 4.

Now suppose $t \geq 6$. Put $d = k-t$, so that (I) gives $v-t+2 \geq d^2+3d+3$ and hence $v-t+4 \geq d^2+3d+5$. Noting $v-2 \geq k-1$, $v-4 \geq k-3$, etc. we deduce from (L) that $(d+5)(d+3)(d+1) \geq (d^2+3d+5)(d^2+3d+3)$, but this is plainly false when $d \geq 2$.

Case (vii). Put $u = t/2$ and $m = k/2$. S-cyclic k-block orbits have difference set of one of the following types:

type 1 $\langle d_1, d_2, \ldots, d_m, d_m, \ldots, d_2, d_1\rangle$,

type 2(a) $\langle d_1, d_2, \ldots, d_{m-1}, e, d_{m-1}, \ldots, d_2, d_1, f\rangle$, e and f both even,

type 2(b) $\langle d_1, d_2, \ldots, d_{m-1}, e, d_{m-1}, \ldots, d_2, d_1, f\rangle$, e and f both odd.

It is easily shown (in the manner of Case (vi)), that each type 1 orbit therefore contains a block of the form

$$\{0, x_1, x_2, \ldots, x_{m-1}, v/2, v-x_{m-1}, \ldots, v-x_2, v-x_1\}$$

where $1 \le x_1 < x_2 < \ldots < x_{m-1} \le (v-2)/2$. Each type 2(a) orbit contains a block of the form

$$\{x_1, x_2, \ldots, x_m, v - x_m, \ldots, v - x_2, v - x_1\}$$

where $1 \le x_1 < x_2 < \ldots < x_m \le (v-2)/2$. Each type 2(b) orbit contains a block of the form

$$\{x_1, x_2, \ldots, x_m, v + 1 - x_m, \ldots, v + 1 - x_2, v + 1 - x_1\}$$

where $1 \le x_1 < x_2 < \ldots < x_m \le (v-2)/2$. Note that a full orbit of type 1 contains at least two blocks of the type quoted above (this may be seen by applying the mapping $z \to z + v/2 \pmod v$). A similar observation applies to types 2(a) and 2(b).

We define symmetric t-blocks of types A and B as follows:

type A: $\{0, \alpha_1, \alpha_2, \ldots, \alpha_{u-1}, v/2, v - \alpha_{u-1}, \ldots, v - \alpha_2, v - \alpha_1\}$,
where $1 \le \alpha_1 < \alpha_2 < \ldots < \alpha_{u-1} \le (v-2)/2$.

or: $\{\alpha_1, \alpha_2, \ldots, \alpha_u, v - \alpha_u, \ldots, v - \alpha_2, v - \alpha_1\}$,
where $1 \le \alpha_1 < \alpha_2 < \ldots < \alpha_u \le (v-2)/2$.

type B: $\{\alpha_1, \alpha_2, \ldots, \alpha_u, v + 1 - \alpha_u, \ldots, v + 1 - \alpha_2, v + 1 - \alpha_1\}$,
where $1 \le \alpha_1 < \alpha_2 < \ldots < \alpha_u \le v/2$.

There are $\binom{v/2}{u}$ symmetric t-blocks of type A and the same number of type B. A full S-cyclic k-block orbit of types 1 or 2(a) will contain at least $2\binom{m}{u}$ symmetric t-blocks of type A. Likewise a full orbit of type 2(b) will contain $2\binom{m}{u}$ sub-blocks of type B. Smaller k-block orbits will contain at least $\binom{m}{u}$ of the respective types. It follows that the number of S-cyclic orbits which can be used to form an $\mathrm{S}(t,k,v)$ expressed in equivalent full orbits (i.e. an orbit of cardinality v/n contributing $1/n$ towards the total) is at most

$$\binom{v/2}{u}\Big/2\binom{m}{u} + \binom{v/2}{u}\Big/2\binom{m}{u} = \binom{v/2}{u}\Big/\binom{m}{u}.$$

$$\text{Hence } \binom{v/2}{u}\Big/\binom{m}{u} \ge \binom{v}{t}\Big/\left(v\binom{k}{t}\right).$$

This reduces to $(k-1)(k-3)\ldots(k-t+1) \ge (v-1)(v-3)\ldots(v-t+1)/v$ which we call (M).

When $t = 4$ this gives $(k-1)(k-3) \ge (v-1)(v-3)/v$. Noting $v > k$ gives $(v-1)/v = 1 - 1/v > 1 - 1/k$ and so $k(k-3) > v - 3$, hence $v < k^2 - 3k + 3$, From this and (I) we deduce that $k^2 - 5k + 9 \le v \le k^2 - 3k + 2$. But k and

v are even and $(k-3)|(v-3)$, so that the possible values of v are reduced simply to $v = k^2 - 4k + 6$, The existence of $\mathrm{S}(4, k, k^2 - 4k + 6)$ implies that $k|(k^2 - 4k + 6)(k^2 - 4k + 5)(k - 2)$ so that $k|60$. But k is even and $k \geq 6$, so the possible values of k are $k = 6, 10, 12, 20, 30$ and 60. However, these systems are all extendable inversive planes, the last four being ruled out by a theorem of Dembowski [2], [3]. It is well-known that no system $\mathrm{S}(4, 6, 18)$ exists (Witt [12]), and the non-existence of $\mathrm{S}(4, 10, 66)$ can be deduced from work by Kantor [9], (see also [1] and [4]).

Now suppose $t \geq 6$. Put $d = k - t$, so that (I) gives $v - t + 1 \geq d^2 + 3d + 2$. Noting $v - 3 \geq k - 1$, $v - 5 \geq k - 3$ etc., we deduce from (M) that $(d+5)(d+3)(d+1) \geq (d^2+3d+4)(d^2+3d+2)(v-1)/v$. But $\frac{v-1}{v} \geq 1 - \frac{1}{k+2} \geq 1 - \frac{1}{10} = \frac{9}{10}$. Hence $10(d + 5)(d + 3)(d + 1) \geq 9(d^2 + 3d + 4)(d^2 + 3d + 2)$. This is plainly false for $d \geq 2$.

Case (viii). Put $u = (t-1)/2$ and $m = k/2$. The S-cyclic k-block orbits are as in Case (vii) and the observations concerning them which we made there still apply. We define symmetric t-blocks of types A and B as follows:

type A: $\{0, \alpha_1, \alpha_2, \ldots, \alpha_{u-1}, v/2, v - \alpha_{u-1}, \ldots, v - \alpha_2, v - \alpha_1, \gamma\}$,
where $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_{u-1} \leq (v-2)/2$,
$1 \leq \gamma \leq (v-2)/2$.

or: $\{\alpha_1, \alpha_2, \ldots, \alpha_u, v - \alpha_u, \ldots, v - \alpha_2, v - \alpha_1, \gamma\}$,
where $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_u \leq (v-2)/2$,
$0 \leq \gamma \leq (v-2)/2$.

type B: $\{\alpha_1, \alpha_2, \ldots, \alpha_u, v + 1 - \alpha_u, \ldots, v + 1 - \alpha_2, v + 1 - \alpha_1, \gamma\}$,
where $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_u \leq v/2$, $1 \leq \gamma \leq v/2$.

There are $\frac{v}{2}\binom{(v-2)/2}{u}$ symmetric t-blocks of type A and the same number of type B. A full S-cyclic k-block orbit of types 1 or 2(a) will contain at least $2m\binom{m-1}{u}$ symmetric t-blocks of type A. Likewise a full orbit of type 2(b) will contain at least $2m\binom{m-1}{u}$ sub-blocks of type B. Smaller k-block orbits will contribute at least $m\binom{m-1}{u}$ of the respective types. It follows that the number of S-cyclic orbits which can be used to form an $\mathrm{S}(t, k, v)$, expressed in equivalent full orbits is at most

$$\frac{\frac{v}{2}\binom{(v-2)/2}{u}}{2m\binom{m-1}{u}} + \frac{\frac{v}{2}\binom{(v-2)/2}{u}}{2m\binom{m-1}{u}} = \frac{v}{2m} \cdot \frac{\binom{(v-2)/2}{u}}{\binom{m-1}{u}}.$$

Hence the existence of an S-cyclic system implies that

$$\frac{v}{2m} \cdot \frac{\binom{(v-2)/2}{u}}{\binom{m-1}{u}} \geq \frac{\binom{v}{t}}{v\binom{k}{t}}.$$

This reduces to

$(k-1)(k-3)\ldots(k-t+2) \geq (v-1)(v-3)...(v-t+2)/v,$ which we call (N).

When $t = 5$ this gives $(k-1)(k-3) \geq (v-1)(v-3)/v$. Arguing as in Case (vii) and using (I) gives $k^2 - 7k + 16 \leq v \leq k^2 - 3k + 2$. Since $(k-4)|(v-4)$ this gives the possible values of v as $v = k^2 - 7k + 16$, $v = k^2 - 6k + 12$, $v = k^2 - 5k + 8$, $v = k^2 - 4k + 4$, $v = k^2 - 3k$, and if $k = 6$, $v = k^2 - 2k - 4 = 20$. We examine each of these possibilities below using the admissibility condition and bearing in mind that k is even and $k \geq 6$.

(a) $v = k^2 - 7k + 16$. We require $(k-2)|(k^2 - 7k + 13)(k^2 - 7k + 14)$ and so $(k-2)|12$. Also $(k-1)|(k^2 - 7k + 13)(k^2 - 7k + 14)(k^2 - 7k + 15)$ and so $(k-1)|7 \times 8 \times 9$. The only solution to these two divisibility conditions is $k = 8$ which gives $v = 24$. However, the system $\mathrm{S}(5, 8, 24)$ is not cyclic.

(b) $v = k^2 - 6k + 12$. We require $(k-1)|(k-3)(k^2 - 6k + 10)(k^2 - 6k + 11)$ so that $(k-1)|60$, and $k|(k-3)(k^2 - 6k + 10)(k^2 - 6k + 11)(k^2 - 6k + 12)$ so that $k|3 \times 10 \times 11 \times 12$. The only solution is $k = 6$ which gives $v = 12$. The system $\mathrm{S}(5, 6, 12)$ is not cyclic.

(c) $v = k^2 - 5k + 8$. We require $(k-3)|(k-1)(k^2 - 5k + 5)$ so that $(k-3)|2$, which is not possible.

(d) $v = k^2 - 4k + 4$. We require $(k-3)|k(k^2 - 4k + 1)$ so that $(k-3)|6$. The only solution is $k = 6$ which gives $v = 16$, but there is no Steiner system $\mathrm{S}(5, 6, 16)$, [11].

(e) $v = k^2 - 3k$. We require $(k-3)|(k+1)(k^2 - 3k - 3)$ so that $(k-3)|12$. The only solution is $k = 6$ which gives $v = 18$. If an S-cyclic $\mathrm{S}(5, 6, 18)$ did exist, then by taking the blocks containing 0 and deleting this element we should obtain a derived $\mathrm{S}(4, 5, 17)$ fixed by $z \to 18 - z$ (mod 18). However, Denniston has shown [4], that any $\mathrm{S}(4, 5, 17)$ must have the trivial automorphism group. Consequently there is no S-cyclic $\mathrm{S}(5, 6, 18)$.

(f) $k = 6$, $v = k^2 - 2k - 4 = 20$. The parameters $(5, 6, 20)$ are not admissible.

Next we consider the situation when $7 \leq t \leq 13$. We put $d = k - t$ and use (I) and (N) together with the inequalities $v - 3 \geq k - 1$ etc. to obtain

$$(d+6)(d+4)(d+2) \geq \left(\frac{v-1}{v}\right)(d^2+3d+5)(d^2+3d+3).$$

But $(v-1)/v \geq 9/10$ and so this gives

$$10(d+6)(d+4)(d+2) \geq 9(d^2+3d+5)(d^2+3d+3).$$

Noting d is odd, this can only hold for $d = 1$. Hence the possibilities are: $t = 7, k = 8$; $t = 9, k = 10$; $t = 11, k = 12$; $t = 13, k = 14$. We examine each in turn.

(a) If $t = 7$ and $k = 8$, then (N) gives $7\times5\times3 \geq (v-1)(v-3)(v-5)/v$ while (I) gives $v \geq 12$. Since $2|v$ the only solutions possible are $v = 12$ and $v = 14$. But neither $(7, 8, 12)$ nor $(7, 8, 14)$ are admissible parameter sets.

(b) If $t = 9$ and $k = 10$ then (N) and (I) give $v = 14$ and $(9, 10, 14)$ is inadmissible.

(c) If $t = 11$ and $k = 12$ then (N) and (I) give $v = 16$, again inadmissible.

(d) If $t = 13$ and $k = 14$ then (N) and (I) give $v = 18$, again inadmissible.

Finally we consider the situation when $t \geq 15$. Then (N) and (1) together with the inequalities $v - 1 \geq k - 3$ etc., give

$$(d+14)(d+12)\ldots(d+2) \geq \left(\frac{v-1}{v}\right)(d^2+3d+13)(d^2+3d+11)\ldots(d^2+3d+3)$$

but $(v-1)/v \geq 17/18$ and so

$$18(d+14)(d+12)\ldots(d+2) \geq 17(d^2+3d+13)(d^2+3d+11)\ldots(d^2+3d+3)$$

and this is false for $d \geq 1$.

3 Construction of $\mathbf{S}(3, 5, 17)$

It is well known that a Steiner system with parameters $t = 3$, $k = 5$, $v = 17$ is unique up to isomorphism, [12]. It is also S-cyclic [5] and the use of this fact provides a simple construction of the system. We first observe that every cyclic orbit is full in this case and that 4 cyclic 5-block orbits are required. Each of the cyclic 5-block orbits will contain all of the blocks in 10 cyclic 3-block orbits. In standard form an S-cyclic 5-block orbit has a difference set of the form $\langle a, b, c, b, a\rangle$ with $2a + 2b + c = 17$. The cyclic 3-block orbits which it contains then have the following difference sets:

1 : $\langle a, b, a + b + c\rangle$ 2. $\langle b, a, a + b + c\rangle$ 3. $\langle b, c, 2a + b\rangle$
4. $\langle c, b, 2a + b\rangle$ 5. $\langle a, b + c, a + b\rangle$ 6. $\langle a, a + b, b + c\rangle$
7. $\langle b, b + c, 2a\rangle$ 8. $\langle b, 2a, b + c\rangle$ 9. $\langle a, a, 2b + c\rangle$
10. $\langle a + b, a + b, c\rangle$.

For any S-cyclic 5-block orbit which can be used as part of S$(3, 5, 17)$,these 10 difference sets must be distinct, and so a number of inequalities immediately follow for such a 5-block orbit.

From 1 and 2, $a \neq b$.

From 3 and 4, $b \neq c$, $2a + b \neq c$.

From 5 and 6, $a \neq c$, $a \neq b + c$.

From 7 and 8, $2a \neq b + c$, $b \neq 2a$.

Next we list all S-cyclic 5-block orbits indicating those which can be used to construct S$(3, 5, 17)$ by an upper case letter and those which can not by the condition which renders them unsuitable.

$\langle 1, 1, 13, 1, 1\rangle$	$a = b$	$\langle 3, 2, 7, 2, 3\rangle$	H
$\langle 1, 2, 11, 2, 1\rangle$	$b = 2a$	$\langle 3, 3, 5, 3, 3\rangle$	$a = b$
$\langle 1, 3, 9, 3, 1\rangle$	A	$\langle 3, 4, 3, 4, 3\rangle$	$a = c$
$\langle 1, 4, 7, 4, 1\rangle$	B	$\langle 3, 5, 1, 5, 3\rangle$	$2a = b + c$
$\langle 1, 5, 5, 5, 1\rangle$	$b = c$	$\langle 4, 1, 7, 1, 4\rangle$	$2a = b + c$
$\langle 1, 6, 3, 6, 1\rangle$	C	$\langle 4, 2, 5, 2, 4\rangle$	I
$\langle 1, 7, 1, 7, 1\rangle$	$a = c$	$\langle 4, 3, 3, 3, 4\rangle$	$b = c$
$\langle 2, 1, 11, 1, 2\rangle$	D	$\langle 4, 4, 1, 4, 4\rangle$	$a = b$
$\langle 2, 2, 9, 2, 2\rangle$	$a = b$	$\langle 5, 1, 5, 1, 5\rangle$	$a = c$
$\langle 2, 3, 7, 3, 2\rangle$	$2a + b = c$	$\langle 5, 2, 3, 2, 5\rangle$	$a = b + c$
$\langle 2, 4, 5, 4, 2\rangle$	$b = 2a$	$\langle 5, 3, 1, 3, 5\rangle$	J
$\langle 2, 5, 3, 5, 2\rangle$	E	$\langle 6, 1, 3, 1, 6\rangle$	K
$\langle 2, 6, 1, 6, 2\rangle$	F	$\langle 6, 2, 1, 2, 6\rangle$	L
$\langle 3, 1, 9, 1, 3\rangle$	G	$\langle 7, 1, 1, 1, 7\rangle$	$b = c$

For the 12 5-block orbits A to L, we list the two values of x, namely a and $a+b$, for which they contain 3-block orbits with a difference set $\langle x, x, 17-x\rangle$.

A	1 and 4	G	3 and 4
B	1 and 5	H	3 and 5
C	1 and 7	I	4 and 6
D	2 and 3	J	5 and 8
E	2 and 7	K	6 and 7
F	2 and 8	L	6 and 8

It is then immediate that the only possible combinations of orbits to form an $\mathrm{S}(3,5,17)$ are as follows:

1.	A	D	J	K
2.	A	E	H	L
3.	A	F	H	K
4.	B	E	G	L
5.	B	F	G	K
6.	C	D	I	J
7.	C	F	H	I

However, orbit A with difference set $\langle 1,3,9,3,1\rangle$ includes inter alia the 3-block orbits with difference sets $\langle 1,3,13\rangle$ and $\langle 3,9,5\rangle$. But orbit H with difference set $\langle 3,2,7,2,3\rangle$ also includes the 3-block orbit with difference set $\langle 3,9,5\rangle$ and orbit K with difference set $\langle 6,1,3,1,6\rangle$ includes the 3-block orbit with difference set $\langle 1,3,13\rangle$. Hence possibilities 1., 2., and 3. are not solutions. Similarly orbit F with difference set $\langle 2,6,1,6,2\rangle$ includes 3-block orbits with difference sets $\langle 1,6,10\rangle$ and $\langle 2,7,8\rangle$, these also being included in orbits K and H respectively. Hence neither possibility 5. nor 7. is a solution.

We are left with just two possibilities and a listing of all the 3-block orbits which each contains verifies that each is indeed an $\mathrm{S}(3,5,17)$. That the two systems are isomorphic is shown by the fact that the function $z \to 3z$ (3 is a primitive of 17) maps the orbits of one system to the orbits of the other. A listing of the difference sets of the orbits of the two systems and the effect of the function is given below:

$$\begin{tikzcd}
\langle 1,4,7,4,1\rangle\ \mathrm{B} \arrow[d] & \langle 6,2,1,2,6\rangle\ \mathrm{L} \arrow[d] & \langle 3,1,9,1,3\rangle\ \mathrm{G} \arrow[d] & \langle 2,5,3,5,2\rangle\ \mathrm{E} \arrow[d] \\
\langle 2,1,11,1,2\rangle\ \mathrm{D} \arrow[ur] & \langle 1,6,3,6,1\rangle\ \mathrm{C} \arrow[ur] & \langle 5,3,1,3,5\rangle\ \mathrm{J} \arrow[ur] & \langle 4,2,5,2,4\rangle\ \mathrm{I} \arrow[ulll]
\end{tikzcd}$$

REFERENCES

1. P. J. Cameron, *Extremal Results and Configuration Theorems for Steiner systems*, Annals of Discrete Math. 7 (1980), 43–63.

2. P. Dembowski, *Möbiusebenen gerader Ordnung*, Math. Ann. 157 (1964), 179–205.

3. P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin-Heidelberg-New York (1968).

4. R. H. F. Denniston, *The problem of the higher values of t*, Annals of Discrete Math. 7 (1980), 65–70.

5. I. Diener, *On S-cyclic Steiner systems*, Discrete Math. 39 (1982), 283–292.

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

7. M. J. Grannell and T. S. Griggs, *On the structure of S-cyclic Steiner quadruple systems*, Ars Combinatoria 9 (1980), 51–58.

8. M. J. Grannell and T. S. Griggs, *Some recent results on cyclic Steiner quadruple systems - a survey*, Annals of Discrete Math. 18 (1983), 409–418.

9. W. M. Kantor, *Dimension and embedding theorems for geometric lattices*, J. Combinatorial Theory (A) 17 (1974), 173–195.

10. E. Köhler, *Zyklische Quadrupelsysteme*, Abh. Math. Sem. Univ. Hamburg, 48 (1979), 1–24.

11. N. S. Mendelsohn and S. H. Y. Hung, *On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$*, Utilitas Math. 1 (1972), 5–95.

12. E. Witt, *Über Steinersche Systeme*, Abh. Math. Sem. Univ. Hamburg, 12 (1938), 265–275.