Math. Z. 139, 87–104 (1974)

Intersection Triangles and Block Intersection Numbers of Steiner Systems

Benedict H. Gross

A Steiner system $S(t, k, v)$ is a collection of k-subsets, called blocks, of a v-set of points with the property that any t-subset of points is contained in a unique block. For any block B of $S(t, k, v)$ and for i in the range $0 \leqq i \leqq t-1$ we let x_i denote the number of blocks of S meeting B in precisely i points. Mendelsohn [7] demonstrated that the values of the x_i depend only on the parameters (t, k, v) of S, and not on the particular block B chosen. In this paper we continue an investigation begun by Noda [9] and determine all the possible parameter sets (t, k, v) for a Steiner system with the property that $x_0 = 0$, that is—that any two blocks of $S(t, k, v)$ have non-trivial intersection. They are:

1. $(t, k, v) = (2, n+1, n^2+n+1)$ and S is a projective plane,

2. $(t, k, v) = (4, 7, 23)$ and S is the unique system with these parameters first discovered by Witt [11], or

3. $(t, k, v) = (t, t+1, 2t+3)$ and $t+3$ is a prime number.

We then extend this result slightly to characterize those Steiner systems with $x_i = 0$ for any $i < t$.

1. Putative Parameter Sets and their Intersection Triangles

A central question in the study of Steiner systems is this: given a set of integral parameters (t, k, v) with the additional stipulation that $2 \leqq t < k \leqq v-2$ (to avoid certain trivial configurations), when does a Steiner system $S(t, k, v)$ with such parameters exist? The following two lemmas provide us with some strong "existence" criteria.

Lemma 1. *Let S be a Steiner system with parameters (t, k, v) and let i be an integer with $0 \leqq i \leqq t$. Then the number of blocks of S containing any i-set of points is a constant depending only on the parameter set (t, k, v) and not on the particular i-set of points chosen. If we call this constant λ_i we have the formula: $\lambda_i = \binom{v-i}{t-i} \Big/ \binom{k-i}{t-i}$.*

Proof. If $X = \{v_1, v_2, \ldots, v_i\}$ is our specific i-set of points we count the number of elements in the set $\{(Y, B)$: Y is a t-set containing X and B is a block containing $Y\}$ in two ways. First we count the number of such t-sets Y containing X and note that each Y is contained in a unique block B. This gives $\binom{v-i}{t-i}$ members. But we can also start by counting all the blocks B containing X and then make Y up from the remaining points in these blocks. This gives $\lambda_i(X)\cdot\binom{k-i}{t-i}$ members, where $\lambda_i(X)$ is the number of blocks containing X. Equating the two gives the independence of λ_i from the set X and the formula of our lemma.

Lemma 2. *Let S be a Steiner system with parameters $(2, k, v)$ with $b=\lambda_0=$ the number of blocks of S. Then $b \geqq v$. Further, $b=v$ if and only if every two blocks have a non-trivial intersection. S is then a projective plane with parameters $(2, n+1, n^2+n+1)$.*

Proof. Take a block B and a point p not contained in B. The k blocks joining p to points of B are all distinct and have only the point p in common; hence $v \geqq k(k-1)+1$. But using the formula for $b=\lambda_0$ given by Lemma 1 shows $b=v(v-1)/k(k-1)$; thus we see that $b \geqq v$. If equality holds we must have $v=k(k-1)+1$ which is equivalent to the statement that every block through p meets B; since p and B were arbitrary this is equivalent to the statement that any two blocks meet.

Note. Lemma 2 is a restricted form of Fisher's inequality which is valid in any balanced incomplete block design. This inequality has recently been extended by Wilson and Ray-Chaudhuri [10]. But, as I will show a bit later, their result gives no new existence tests for Steiner systems beyond that of Fisher's inequality.

To use these two lemmas as existence tests on a set (t, k, v) of possible parameters, we note that the first result requires that for $0 \leqq i \leqq t$ the rational numbers $\binom{v-i}{t-i}\Big/\binom{k-i}{t-i}$ must in fact be integers, as they count the number of blocks containing a given set of i points. We call the conditions imposed by Lemma 1 the "divisibility conditions". To employ the second result we must first define the notion of the contraction of a Steiner system. Suppose we have a Steiner system with parameters $S(t, k, v)$ on the point set V; if we take any i-set of points, say $\{v_1, v_2, \ldots, v_i\}$, with $0 \leqq i \leqq t$ and consider the configuration with point set $V-\{v_1, \ldots, v_i\}$ and blocks the λ_i blocks of $S(t, k, v)$ containing $\{v_1, \ldots, v_i\}$ we get a new Steiner system with parameters $S(t-t, k-i, v-i)$ which we call the i-th contraction of S with respect to the set $\{v_1, \ldots, v_i\}$. Frequently, the isomorphism class of $S(t-i, k-i, v-i)$ depends on the particular i-set of points chosen. But the set of parameters is clearly the same for any i-th contraction. To use Lemma 2 we note that if a Steiner system with parameters (t, k, v) exists, then so does its $(t-2)$-nd contraction with parameters $(2, k-t+2, v-t+2)$, and the contracted system must satisfy Fisher's inequality.

Although there are a few specialized results on the existence of Steiner systems with certain parameter sets (see, for example, the theorems of Kantor [6] and Dembowski [3, 4] on extensions of affine planes), Fisher's inequality and the divisibility conditions are the most powerful general tests available. So, in this paper I will observe the following convention: (t, k, v) will be called a "putative parameter set" for a Steiner system if

1. $2 \leqq t < k \leqq v-2$.

2. For $0 \leqq i \leqq t$ the numbers $\binom{v-i}{t-i} \Big/ \binom{k-i}{t-i}$ are rational integers.

3. The inequality $(v-t+1) \geqq (k-t+1)(k-t+2)$ holds.

We now present a slight extension of Lemma 1 which leads us to the construction of an "intersection triangle" for any $S(t, k, v)$.

Lemma 3. *Let S be a Steiner system with parameters (t, k, v) and let V_i and V_j be an i-set and a j-set of points respectively, satisfying*

1. $V_i \cap V_j = \varnothing$.
2. *There is a block B of S containing $V_i \cup V_j$.*

Then the number of blocks of S which contain V_i and are disjoint form V_j is determined solely by the values of i and j and the parameters of the design. It is independent of the particular i- and j-sets chosen.

Proof. Set $\lambda_{i,j}(V_i, V_j)$ be the number of blocks of S with this property. We prove the lemma by induction on j; for $j=0$ and $0 \leqq i \leqq t$ we have λ_{i0} well determined independent of the set V_i by the results of Lemma 1. For $j=0$ and $t \leqq i \leqq k$ we must, by the definition of S, have $\lambda_{i0}=1$. Now let p be a point in V_j; we have the recursion $\lambda_{i,j}(V_i, V_j) = \lambda_{i,j-1}(V_i, V_j - p) - \lambda_{i+1,j-1}(V_i + p, V_j - p)$. Using induction on j, we see the right side of this equation is well determined independent of the specific sets of points chosen; hence the left side is also. We write this integer just as $\lambda_{i,j}$; it is clearly non-negative.

Does Lemma 3 give us any further existence tests on putative parameter sets? As the $\lambda_{i,j}$ are all obtained by successive subtractions from the $\lambda_{i,0}$, which by our assumptions are integers, they will all have integral values. But it is possible that a putative parameter set might yield a negative value for one of the $\lambda_{i,j}$; this would clearly eliminate it from contention. For example, a quick glance at Lemma 2 shows that the non-negativity of $\lambda_{t-2,k-t+2}$ is equivalent to the contracted system $S(2, k-t+2, v-t+2)$ satisfying Fisher's inequality. In fact, we will show that any putative parameter set has non-negative entries in its entire intersection triangle; by this we mean the configuration obtained by setting

$$\lambda_{i,0} = \binom{v-i}{t-i} \Big/ \binom{k-i}{t-i} \quad \text{for } 0 \leqq i \leqq t.$$

$$\lambda_{i,0} = 1 \quad \text{for } t \leqq i \leqq k.$$

$$\lambda_{i,j} = \lambda_{i,j-1} - \lambda_{i+1,j-1} \quad \text{for } j \geqq 1,\ 1 \leqq i+j \leqq k$$

and represented visually as a triangle, viz.

$$\begin{array}{ccccccc} & & & \lambda_{0,0} & & & \\ & & \lambda_{0,1} & & \lambda_{1,0} & & \\ & \lambda_{0,2} & & \lambda_{1,1} & & \lambda_{2,0} & \\ & & & \text{etc.} & & & \\ \lambda_{0,k} & \lambda_{1,k-1} & & & & \lambda_{k-1,1} & \lambda_{k,0} \end{array}$$

Although, for any putative parameter set, this triangle will turn out to be non-negative, giving us no new existence tests, we may enquire whether any of the entries are zero. If we consider the properties of the Steiner system our system of parameters hopes to represent, we can see immediately that $\lambda_{i,j}=0$ whenever $t+1\leqq i\leqq k$ and $j>0$. But we may also get zero entries in various non-trivial places in our intersection triangle; consider the triangle generated by the parameter set (5, 8, 24):

759								
506	253							
330	176	77						
210	120	56	21					
130	80	40	16	5				
78	52	28	12	4	1			
46	32	20	8	4	0	1		
30	16	16	4	4	0	0	1	
30	0	16	0	4	0	0	0	1

Notice that $\lambda_{1,k-1}=\lambda_{3,k-3}=0$. Recalling the definition of the block intersection numbers x_i given in the first paragraph, it is easy to see that $x_i=\lambda_{i,k-i}\binom{k}{i}$. Thus, from the vanishing of elements in the intersection triangle of (5, 8, 24) we may infer that in any Steiner system with such parameters, blocks may only intersect in 0, 2, 4, or 8 points. This is an extremely valuable piece of information; in fact, given the existence of an $S(5,8,24)$ we can use this result, with very little else, to demonstrate its uniqueness. Thus it seems reasonable to ask what other putative parameter sets may have vanishing intersection numbers; we answer this question in our next section.

2. Statement of Results

Let us first note that in investigating the non-negativity of elements in the intersection triangle of (t, k, v) we may begin by concentrating our attention on the bottom row, where $i+j=k$.

Lemma 4. *If $\lambda_{i,k-i}\geqq 0$ for all i, then $\lambda_{i,j}\geqq 0$ for all i and j.*

Proof. We do a backwards induction on i. The lemma is clearly true for $i=k$. If the lemma first fails for $\lambda_{i,j}<0$, then by our recursion

$$\lambda_{i,j+1}=\lambda_{i,j}-\lambda_{i+1,j}<0 \quad \text{as} \quad \lambda_{i+1,j}\geqq 0 \quad \text{by induction.}$$

Similarly,

$$\lambda_{i,j+2}=\lambda_{i,j+1}-\lambda_{i+1,j+1}<0.$$

Continuing in this manner gives $\lambda_{i,k-i}<0$, a contradiction.

Furthermore, in examining the values of the bottom row we may restrict our attention still further to the value of $\lambda_{0,k}$ for an arbitrary putative parameter set (t, k, v). For if we are interested in the value of $\lambda_{i,k-i}$ we just look at $\lambda'_{0,k-i}$ of the i-th contraction $(t-i, k-i, v-i)$. Notice that $\lambda_{0,k}=x_0=$the number of blocks disjoint from a given block in an $S(t, k, v)$. Hence, if for a putative parameter set we have $x_0=0$, then any Steiner system with those parameters must be such that every two blocks meet. The following result, and its corollaries, settles the question of non-negative and zero entries in the intersection triangle of any putative parameter set.

Theorem 1. *Let (t, k, v) be a putative parameter set for a Steiner system, and let $x_0=\lambda_{0,k}$ be the value obtained from its intersection triangle by successive subtractions. Then $x_0 \geqq 0$. If $x_0=0$ then*

1. $(t, k, v)=(2, n+1, n^2+n+1)$.
2. $(t, k, v)=(4, 7, 23)$.
3. $(t, k, v)=(t, t+1, 2t+3)$ *and* $t+3$ *is a prime number.*

Corollary 1. *Let (t, k, v) be a putative parameter set for a Steiner system with $x_i=\binom{k}{i}\lambda_{i,k-i}$ the value of its "block intersection" numbers obtained by successive subtractions from its intersection triangle. Then $x_i \geqq 0$. If $x_i=0$ then*

1. $i=0$ *and* (t, k, v) *as in Theorem* 1.
2. $i=1$ *and* $(t, k, v)=(3, 4, 8)$
   $(3, 6, 22)$
   $(3, 12, 112)$
   $(5, 8, 24)$
   $(t, t+1, 2t+2)$ *and* $t+2$ *is a prime number.*
3. $i=2$ *and* $(t, k, v)=(4, 7, 23)$.
4. $i=3$ *and* $(t, k, v)=(5, 8, 24)$.

Proof (of Corollary). If $x_i<0$ then $\lambda_{i,k-i}<0$, likewise. But then x'_0 of the i-th contraction is less than zero, which contradicts Theorem 1.

Similarly, if $x_i=0$ we have x'_0 of the i-th contraction equal to zero also, so it must be one of the cases of Theorem 1. It remains to see how far the putative parameter sets of Theorem 1 may be extended. In the first case, when $(t, k, v)=(2, n+1, n^2+n+1)$, it is well known that the first extension fails the divisibility conditions unless $n=2, 4$, or 10. Only the $(2, 5, 21)$ set may be extended more than once; it may be extended to $(5, 8, 24)$ before it fails the divisibility conditions. In the case when $(t, k, v)=(t, t+1, 2t+3)$, it is also easy to check that we may extend precisely once before the divisibility conditions fail (because $t+3$ is a prime). This completes the proof of the corollary.

Note. The existence of Steiner systems with parameters $S(t, k, v)$ where (t, k, v) is one of the putative parameter sets of the previous corollary is a difficult question and is still far from being solved. Here we review some of the knowledge to date. Projective planes $S(2, n+1, n^2+n+1)$ are known to exist when n is a prime power; they do *not* exist when $n\equiv 1$ or 2 (mod 4) but n is not the sum of two squares, Bruck and Ryser [2]. None are *known* to exist when n is not a prime power. The $(3, 4, 8)$ and $(3, 6, 22)$ systems exist and are unique up to isomorphism; Witt [11] demonstrated that the same was true for the $(4, 7, 23)$ and the $(5, 8, 24)$ extensions. Although we have a certain amount of information about possible systems with parameters $(t, t+1, 2t+3)$ it is not known whether any exist for $t>4$. Mendlesohn and Hung [8] have ruled out the next case, $t=8$, by an extensive computer search. Alltopp [1] demonstrated, in a more general theorem, that an $S(t, t+1, 2t+3)$ system exists if and only if its first extension, an $S(t+1, t+2, 2t+4)$ also exists, and that the extension is unique. It is not difficult to show that the extended system cannot have a block transitive automorphism group for $t>4$, though such transitivity was hardly to be expected.

Of course, there is the highly suggestive point that the only Steiner systems we know to exist with $t \geqq 4$ all have some zero intersection numbers.

Corollary 2. *If a Steiner system $S(t, k, v)$ has two (non-trivial) zero intersection numbers it is $S(4, 7, 23)$ or $S(5, 8, 24)$. No Steiner system has three or more (non-trivial) zero intersection numbers.*

Corollary 3. *The intersection triangle for any putative parameter set is always non-negative. It is always strictly positive (except for the trivial zero places) above the bottom row.*

Proof. The first statement follows directly from Corollary 1 and Lemma 4. To demonstrate the positivity of the non-trivial entries above the bottom row, i.e. when $0 \leqq i+j \leqq k$ and $i \leqq t-1$, we argue as in Lemma 4 using a backwards induction on i. Clearly $\lambda_{t-1,j}>0$ for all j. It is easy to see that if $\lambda_{i,j}$ is the first case where, with our assumptions, we get a zero entry, then we must have $j=k-i+1$ and $\lambda_{i,k-i}=\lambda_{i+1,k-i+1}=0$. This gives us two consecutive zeroes in non-trivial places of the bottom row. By Corollary 2 this is impossible.

In the course of the proof of Theorem 1 we make use of a lemma which is concerned with putative parameter sets which have $v<4k$. Since this seemed to be an interesting enough result on its own, we have elevated it to the status of:

Theorem 2. *Let (t, k, v) be a putative parameter set for a Steiner system. Then:*

1. *If $v \leqq 2k+t+1$ then $k=t+1$.*
2. *If $v \leqq 3k+t+2$ then $k \leqq t+2$ unless $(t, k, v)=(3, 6, 22)$, $(4, 7, 23)$ or $(5, 8, 24)$.*

I will defer the proof of this theorem, like that of Theorem 1, to a later section of this paper. Here I will simply state and prove some of its useful corollaries.

Corollary 4. *Let (t, k, v) be a putative parameter set with $v<3k$. Then $k=t+1$.*

Proof. Using part 2 of Theorem 2 we see that $k \leqq t+2$. But if $k=t+2$ then we have $v \leqq 3k-1=2k+(k-1)=2k+t+1$ and we may apply part 1 of the theorem.

Corollary 5. *Let (t, k, v) be a putative parameter set. Then $v \geqq 2k$. If $v=2k$ then $k+1$ is a prime number.*

Proof. By the theorem we must have $k=t+1$ if $v<2k$. By the divisibility conditions we know that $(v-i)(v-i-1)\dots(v-k+2)/(k-i)(k-i-1)\dots2$ is an integer for all i in the range $0 \leqq i \leqq t-1$. Hence, no prime numbers from 2 to k can divide $(v-k+1)$. In particular, $(v-k+1) \geqq k+1$ and so $v \geqq 2k$. If $v=2k$ then $v-k+1=k+1$ must be prime.

Corollary 6. *Let (t, k, v) be a putative parameter set with $v \leqq (11/3)k$ and $t \geqq 3(k-t)$. Then $k \leqq t+2$.*

Proof. As $t \geqq 3(k-t)$ we have $(4/3)t \geqq k$. Hence $v \leqq (11/3)k \leqq (8/3)k+(4/3)t < 3k+t$ as $t<k$.

Hence we may apply part two of Theorem 2.

Finally, I would like to prove a result which is not directly in the line of argument of this paper, but which reinforces its contention that for Steiner systems Fisher's inequality and the divisibility conditions are the strongest existence tests we may apply to any general set of putative parameters. As I mentioned earlier, Wilson and Ray Chaudhuri [10] have generalized Fisher's inequality to apply to any $S_\lambda(t,k,v)$ design where t was even. They demonstrated that if b is the number of blocks in such a design and $t=2s$, then $b \geqq \binom{v}{s}$. Now if we take any $S_\lambda(t,k,v)$ design and apply this inequality to the $2s$-design we obtain by taking the $(t-2s)$-th contraction, we obtain the following inequality for $s=0,1,\ldots,[\frac{1}{2}t]$:

$$\lambda \geqq \binom{k-t+2s}{2s}\binom{v-t+2s}{s}\Big/\binom{v-t+2s}{2s} = (k-t+2s)!\,(v-t)!/(v-t+s)!\,(k-t)!\,s!.$$

Let us call this inequality I_s and the right side of it $f(s)$. It is natural to inquire which of the inequalities is the strongest, for a given parameter set (t,k,v). The following demonstration is due to P. Cameron.

First we put

$$g(s)=f(s+1)/f(s)=(k-t+2s+2)(k-t+2s+1)/(s+1)(v-t+s+1).$$

For non-negative s, $g(s)$ is greater than or less than unity according as s lies outside or between the roots of the quadratic equation

$$Q(s):=3s^2-(v-4k+3t-4)s+\big((k-t+2)(k-t+1)-(v-t+1)\big)=0.$$

$$Q(s)=0 \quad \text{has real roots iff} \quad v \geqq 4k-3t-2+\big(12(k-t)(k-t-1)\big)^{\frac{1}{2}}.$$

Assume this is so and that, in fact, $v-4k+3t-4 \geqq 0$, which will certainly then be true if $k>t+2$ but even in the case when $k \leqq t+2$ will be true so long as $v>k+7$. Let s_1 be the smaller root of the equation and s_2 the larger. Then

$$\begin{aligned} s_1 \geqq 0 &\quad \text{iff} \quad v \leqq (t-1)+(k-t+2)(k-t+1)=:K_1\\ s_2 \leqq \tfrac{1}{2}t-1 &\quad \text{iff} \quad v \leqq \tfrac{1}{2}t+2k(k-1)/t=:K_2\\ K_1 \leqq K_2 &\quad \text{iff} \quad k \leqq t+\tfrac{1}{2}+\tfrac{1}{2}(6t+1)^{\frac{1}{2}}. \end{aligned}$$

If we compare the sign of $Q(s)$, i.e.—that of $g(s)-1$, with the behavior of the consecutive $f(s)$ we have the following:

Lemma 5. *If $v \leqq 4k-3t-2+\big(12(k-t)(k-t-1)\big)^{\frac{1}{2}}$ then $I_{[\frac{1}{2}t]}$ is the strongest of the inequalities. Otherwise assume either $k>t+2$ or $v>k+7$:*

1. *if $v \leqq \min\{K_1,K_2\}$, then either $I_{1+[s]}$ or $I_{[\frac{1}{2}t]}$ is the strongest;*
2. *if $K_2 \leqq v \leqq K_1$, then $k \geqq t+\frac{1}{2}+\frac{1}{2}(6t+1)^{\frac{1}{2}}$, $v \geqq (5/2)t+3+2(6t+1)^{\frac{1}{2}}$, and $I_{1+[s_1]}$ is the strongest;*
3. *if $K_1 \leqq v \leqq K_2$, then $k \leqq t+\frac{1}{2}+\frac{1}{2}(6t+1)^{\frac{1}{2}}$, $v \leqq (5/2)t+3+2(6t+1)^{\frac{1}{2}}$, and either I_0 or $I_{[\frac{1}{2}t]}$ is the strongest;*
4. *if $v \geqq \max\{K_1,K_2\}$, then I_0 is the strongest.*

Fortunately, the situation greatly simplifies in the case where our t-design is a Steiner system. For there the inequality I_0, which says simply that $\lambda \geqq 1$, is actually attained. Thus it must certainly be the strongest of the inequalities. But which then is the next strongest? We clearly must have $v \geqq K_1 = (t-1)+(k-t+2)(k-t+1)$ as this is just I_1, or Fisher's inequality! If $v \geqq K_2$ we are in case 4 of the lemma and, as a quick examination of the behavior of $g(s)-1$ will show, I_1 must be the next strongest inequality. Thus we have established that Fisher's inequality is the strongest of all the Wilson-Ray Chaudhuri inequalities for a Steiner system unless $v \leqq K_2$. The following corollary to Theorem 2 shows that, except for two exceptional cases, Fisher's inequality is always the strongest we can apply to any putative parameter set (t, k, v).

Corollary 7. *Let (t, k, v) be a putative parameter set for a Steiner system. Then, using the notation of the previous lemma, we have $f(1) > f(s)$ for $s = 2, 3, \ldots, [\frac{1}{2}t]$ except in the cases:*

1. $(t, k, v) = (4, 5, 11), (5, 6, 12)$ *where* $f(2) > f(1)$:
2. $(t, k, v) = (4, 7, 23), (5, 8, 24)$ *where* $f(2) = f(1) = f(0)$.

Hence whenever a parameter set satisfies the divisibility conditions and Fisher's inequality, it satisfies all of the Wilson-Ray Chaudhuri inequalities.

Proof. By the previous lemma, we need only consider the case when $v \leqq K_2$ and thus $v \leqq (5/2)t + 3 + 2(6t+1)^{\frac{1}{2}}$. But if $t > 7$ then we obtain

$$v \leqq 4t + 5 \leqq 3k + t + 2.$$

Theorem 2 now gives us $k \leqq t+2$ for $t > 7$. For $t \leqq 7$ a check through the putative parameter sets of Ganter's catalogue [5] indicated that $v \leqq (5/2)t + 3 + 2(6t+1)^{\frac{1}{2}}$ always forced $k \leqq t+2$ except for the Witt designs $(4, 7, 23)$ and $(5, 8, 24)$. We can check that for those designs $f(2) = f(1) = f(0)$ and then proceed with the assumption that $k \leqq t+2$.

W.l.o.g. we now assume that our parameter set has even t, say $t = 2r$. To show that $f(1) > f(s)$ for all $s = 2, 3, \ldots, r$, it is sufficient to demonstrate that $f(1) > f(r)$. If $k = t+1$ then $f(1) = 6/(v-t+1)$ and

$$\begin{aligned} f(r) &= k!\,(v-2r)!/r!\,(v-r)! \\ &= (r+1)(r+2)/(v-t+1) \cdot k(k-1)\ldots(r+3)/(v-r)(v-r-1)\ldots(v-t+2). \end{aligned}$$

The second fraction on the right of this equation has $(r-1)$ terms in its numerator and in its denominator. If we pair them up consecutively, the largest of the ratios $(k-i)/(v-r-i)$ is the first: $k/(v-r)$. By Corollary 5 we know that $v \geqq 2k$; hence $k/(v-r) \leqq k/(2k-r) = (2r+1)/(3r+2) < 2/3$ and so

$$f(r) < (r+1)(r+2)/(v-t+1) \cdot (2/3)^{r-1}.$$

When $r \geqq 10$ we obtain $(2/3)^{r-1}(r+2)(r+1) < 6$ which gives $f(r) < f(1)$ as desired. For $r \leqq 9$ we may check the situation out easily by hand. The only putative parameter set which arises yielding $f(r) \geqq f(1)$ is the system $(4, 5, 11)$ and hence its extension $(5, 6, 12)$. Both have $f(2) > f(1)$.

The case $k = t+2$ is handled similarly, but here no exceptions arise for small values of r. This completes the proof of the corollary.

3. Proof of Theorem 1

To demonstrate the non-negativity of elements in the intersection triangle we clearly need a manageable formula for $\lambda_{i,j}$. The most natural is that suggested by the sieve method:

$$\lambda_{i,j}=\lambda_i-\binom{j}{1}\lambda_{i+1}+\binom{j}{2}\lambda_{i+2}-\cdots+(-1)^j\lambda_{i+j}$$

where the $\lambda_i=\lambda_{i,0}$ are defined in Lemma 1. But for the purpose of testing the non-negativity of the $\lambda_{i,j}$ this formula is practically useless. Instead, we will use:

Lemma 6. *Let (t, k, v) be a putative parameter set with $\lambda_{i,j}$ the entries in its intersection triangle. Then*

$$\lambda_{i,j}=1\Big/\binom{v-t}{k-t}\cdot\left\{\binom{v-i-j}{k-i}+(-1)^{t+i+1}\sum_{q=0}^{i+j-t-1}\binom{t-i-1+q}{q}\binom{v-i-j+q}{k-t}\right\}.$$

Proof. Entirely technical: as usual we use the recurrence relation on our intersection triangle and perform an induction on j. For $j=0$ and $i\leqq t$ the formula yields:

$$\lambda_{i,0}=\binom{v-i}{k-i}\Big/\binom{v-t}{k-t}=\binom{v-i}{t-i}\Big/\binom{k-i}{t-i}$$

which is correct by our very definition of the intersection triangle. For $j=0$ and $t\leqq i\leqq k$ we must show our formula yields $\lambda_{i,0}=1$, or that:

$$\binom{v-t}{k-t}=\binom{v-i}{k-i}+(-1)^{t+i+1}\sum_{q=0}^{i-t-1}\binom{t-i-1+q}{q}\binom{v-i+q}{k-t}$$

when $i\geqq t$

$$\binom{v-t}{k-t}=\binom{v-i}{k-i}+(-1)^{t+i+1}\sum_{q=0}^{i-t-1}(-1)^q\binom{i-t}{q}\binom{v-i+q}{k-t}$$

using $\binom{-n}{q}=(-1)^q\binom{n+q-1}{q}$

$$\binom{v-t}{k-t}=\binom{v-i}{k-i}+\sum_{r=0}^{i-t-1}(-1)^r\binom{i-t}{r+1}\binom{v-t-1-r}{k-t}$$

setting $r=(i-t-1)-q$.

The last equality, however, is easily proved strictly as a binomial identity under the conditions that $v\geqq k\geqq i\geqq t\geqq 2$; it is vacuously true when $v=k$ and then follows by a simple induction argument on v. So our formula is correct for $\lambda_{i,0}$ for all $i\leqq k$.

We now complete the proof of the lemma with an induction on j. Say the formula holds for $\lambda_{i,j-1}$; it is then easy to check, using our recurrence:

$$\lambda_{i,j}=\lambda_{i,j-i}-\lambda_{i+1,j-1}$$

and a few binomial identities, that the formula also holds for $\lambda_{i,j}$.

In our proof of Theorem 1 we really only need the formula for $\lambda_{0,k}=x_0$. We simplify matters slightly by setting

$$n=(v-k)$$
$$m=(k-t).$$

Furthermore, we note that in the formula of Lemma 6 all of the $\lambda_{i,j}$ have a leading factor of $1\Big/\binom{v-t}{k-t}$; since this will not affect the *sign* of the entries in the intersection triangle, we may, by a pseudo-Littlewood convention, assume

$$1\Big/\binom{v-t}{k-t}=1/2\pi i=1.$$

This gives:

$$x_0=\binom{n}{k}+(-1)^{t+1}\sum_{q=0}^{m-1}\binom{t-1+q}{q}\binom{n+q}{m}. \tag{$*$}$$

The usefulness of this formula becomes apparent as we have the immediate result, which was suggested in Noda's work [9]:

Lemma 7. *If* (t, k, v) *is a putative parameter set and* t *is odd, then* $x_0>0$.

Proof. Looking at our formula $(*)$ we see that as $t+1$ is even, x_0 is a sum of non-negative terms. But the first term of the sum is $\binom{n}{k}=\binom{v-k}{k}$. By Corollary 5, $v\geqq 2k$. Thus this term is $\geqq 1$ and $x_0>0$.

To finish the proof of Theorem 1 we treat the case when t is even in several stages. If $t=2$ we have already seen (Lemma 2) that $x_0\geqq 0$ was equivalent with Fisher's inequality and if $x_0=0$ then (t, k, v) were the parameters of a projective plane. We may thus assume $t\geqq 4$.

If $k=t+1$ then by our formula $(*)$:

$$x_0=\binom{n}{k}-\binom{n}{1} \quad \text{as} \quad m=(k-t)=1,$$
$$=\binom{v-k}{v-2k}-(v-k).$$

By Corollary 5, $v\geqq 2k$. If $v\geqq 2k+2$ then clearly $x_0>0$. If $v=2k$ then by Corollary 5 again, $k+1=t+2$ is a prime number. Hence t is odd and we may apply Lemma 7 to conclude that $x_0>0$. If $v=2k+1$ we indeed get $x_0=0$ as claimed in Theorem 1.

If $k=t+2$ our formula $(*)$ yields:

$$x_0=\binom{v-k}{k}-\binom{v-k}{2}-t\binom{v-k+1}{2}$$
$$>\binom{v-k}{k}-(t+1)\binom{v-k+1}{2}=\binom{v-k}{k}-(k-1)\binom{v-k+1}{2}.$$

I will show, for a putative parameter set, that:

$$\binom{v-k}{k} \geqq (k-1)\binom{v-k+1}{2}, \quad \text{or:}$$

$$\frac{(v-k-1)}{1}\cdot\frac{(v-k-2)}{2}\cdot\ldots\cdot\frac{(v-2k+2)}{(k-2)}\cdot\frac{(v-2k+1)}{(k-1)} \geqq \frac{k(k-1)}{2}\cdot(v-k+1).$$

As $k=t+2$ we may assume, by Corollary 4, that $v \geqq 3k$. Thus all the fractions on the left are greater than or equal to 1. But as $t \geqq 4$ implies $k \geqq 6$ we have the following inequalities holding for the first four fractions:

$$\frac{(v-k-2)}{2} \geqq (k-1); \quad \frac{(v-k-3)}{3} \geqq (2/3)\,k-1 > \tfrac{1}{2}k; \quad \frac{(v-k-4)}{4} \geqq \tfrac{1}{2}k-1.$$

Hence, the product on the left is greater than $(v-k-1)(k-1)(\frac{1}{2}k)(\frac{1}{2}k-1)$ which is certainly greater than $(v-k+1)(k-1)(\frac{1}{2}k)$ as $k \geqq 6$. So for $k=t+2$ we always have $x_0 > 0$.

We now assume that $m=(k-t) \geqq 3$. To handle small values of t we prove a short result which, in most cases, allows us to strengthen Fisher's inequality:

Lemma 8. *If* $(2, k, v)$ *are putative parameters of a Steiner system which is neither a projective plane* $(2, n+1, n^2+n+1)$ *nor an affine plane* $(2, n, n^2)$, *then we have* $(v-1) > (k-1)(k+k^{\frac{1}{2}})$.

Proof. By the divisibility conditions we know that $(v-1)/(k-1)=k+m$, where m is a *non-negative* integer by Fisher's inequality. But it is easy to check that $m=0$ implies the parameters are those of a projective plane; similarly $m=1$ gives us an affine plane. So we may assume $m \geqq 2$. By the second divisibility condition:

$$\frac{\big((k-1)(k+m)-1\big)(k+m)}{k}$$

is an integer. Hence k divides $m(m-1)$; as $m \geqq 2$ we must have $k \leqq m(m-1)$ and thus $m > k^{\frac{1}{2}}$.

Now to see when we may apply the stronger equality of Lemma 8 we need only determine all possible extensions of projective or affine planes. If a projective plane can be extended once, the divisibility conditions give us $n+2 \mid 12$ and hence $n=2, 4$, or 10. If an affine plane can be extended twice the divisibility conditions give $n+2 \mid 60$ so $n=3, 4, 8, 10, 13, 18, 28$ or 58. We then examine the intersection triangles of the maximal possible extensions in each case; the only parameter sets yielding $x_0=0$ are (4, 5, 11) and (4, 7, 23), all others give $x_0>0$. This completes the cases where $x_0=0$ as stated in Theorem 1. We now show that if (t, k, v) is not a symmetric or affine extension and $m=(k-t) \geqq 3$, we have $x_0>0$ for all even $t \geqq 4$. We may then use Lemma 8, which says if (t, k, v) is such a parameter set, then:

$$v-t+1 > (k-t+1)\big(k-t+2+(k-t+2)^{\frac{1}{2}}\big),$$

or in our simpler notation:

$$n > (m+1)^2 + (m+1)^{3/2} \quad \text{which is slightly weaker.} \qquad (**)$$

We are now ready to treat the values $t=4, 6, 8, \ldots, 20$ by hand.

For example, if $t=4$ our formula (*) yields:

$$x_0=\binom{n}{m+4}-\sum_{q=0}^{m-1}\binom{q+3}{q}\binom{n+q}{m}.$$

But because we assume that $(4, k, v)$ is a putative parameter set, the 2nd contraction must satisfy Fisher's inequality; equivalently, we must have

$$\lambda_{2,k-2}=\binom{n}{m+2}-\sum_{q=0}^{m-1}\binom{q+1}{q}\binom{n+q}{m}\geqq 0.$$

We compare the ratio of the positive terms in x_0 and $\lambda_{2,k-2}$ with the ratio of their negative terms: i.e., let

$$R^+=\binom{n}{m+4}\Big/\binom{n}{m+2}=\frac{(n-m-2)(n-m-3)}{(m+4)(m+3)},$$

$$R^-=\sum_{q=0}^{m-1}\binom{q+3}{q}\binom{n+q}{m}\Big/\sum_{q=0}^{m-1}\binom{q+1}{q}\binom{n+q}{m}.$$

I will show that $R^+>R^-$ which will clearly imply that $x_0>0$. We observe that R^- is certainly less than or equal to the largest of the individual ratios

$$\binom{q+3}{q}\binom{n+q}{m}\Big/\binom{q+1}{q}\binom{n+q}{m};$$

here the largest among these ratios occurs when $q=m-1$. Hence:

$$R^-\leqq\binom{m+2}{m-1}\Big/\binom{m}{m-1}=\frac{(m+2)(m+1)}{6}.$$

To show that $R^+>R^-$ I need only show that,

$$6(n-m-2)(n-m-3)>(m+4)(m+3)(m+2)(m+1).$$

But by the "strong Fisher's inequality" (**) we know

$$\begin{aligned}6(n-m-2)(n-m-3)&>6\big(m^2+m-1+(m+1)^{3/2}\big)\big(m^2+m-2+(m+1)^{3/2}\big)\\&>6\big(m^2+(5/2)m\big)\big(m^2+(5/2)m-1\big)\\&>(m+4)(m+3)(m+2)(m+1)\quad\text{for } m\geqq 2.\end{aligned}$$

As we are assuming $m\geqq 3$, we have the last inequality and hence $x_0>0$.

A similar method works for $t=6, 8, \ldots, 20$: we proceed by comparing the positive and negative terms of x_0 with those of $\lambda_{t-2,k-t+2}$ which we know to be positive by Fisher's inequality. We then show that R^- is less than or equal to the ratio of the last terms of the sums, this gives us a simple inequality to prove in order to demonstrate that $R^+>R^-$. For example, in the case $t=6$ we must show:

$$\begin{aligned}&5!\,(n-m-2)(n-m-3)\ldots(n-m-5)\\&\quad>(m+6)(m+5)(m+4)^2(m+3)^2(m+2)(m+1).\end{aligned}$$

As we may apply the "strong Fisher's inequality" we know $n>(m+1)^2+(m+1)^{3/2}$ and the above inequality thus holds for $m\geqq 3$. In the case $t=10$ we must do a bit more work; our task reduces to showing:

$$9!(n-m-2)\dots(n-m-9)$$
$$>(m+10)(m+9)(m+8)^2(m+7)^2\dots(m+3)^2(m+2)(m+1).$$

Using the strong Fisher's this holds for $m\geqq 4$; it also holds for $m=3$ as long as $n\geqq 27$ – the inequality (**) just gives $n\geqq 24$. However if $24\leqq n\leqq 26$ our parameter set must be one of (10, 13, 37), (10, 13, 38), (10, 13, 39); none of these are putative as they all fail the divisibility conditions. Similar methods show $x_0>0$ for all putative parameter sets (t, k, v) with $m=(k-t)\geqq 3$ and $t\leqq 20$.

We split the final stage of the proof ($t\geqq 22$) into two cases. First let us assume that $t<3m$. Here we proceed as above; to show $R^+>R^-$ we must show:

$$(t-1)!(n-m-2)(n-m-3)\dots(n-m-t+1)$$
$$>(m+t)(m+t-1)(m+t-2)^2\dots(m+3)^2(m+2)(m+1).$$

Since we are assuming $t<3m$, all the terms on the left of this expression are greater than $n-4m+1$, which, by the strong Fisher's, is greater than m^2 (as $t>20$ implies $m>7$). Hence the left side is greater than $(t-1)!\,m^{2(t-2)}$. On the right side, however, the largest term is less than $4m$, and at least half the terms are less than $(5/2)m$. Hence the product on the right is less than

$$(5/2)^{t-2}(4)^{t-2}m^{2(t-2)}=10^{t-2}m^{2(t-2)}.$$

To make the left side larger than the right we only need $(t-1)!\geqq 10^{t-2}$; this is true for $t\geqq 22$ as desired. Thus we have shown $x_0>0$ when $t<3m$.

Finally, we assume that $t>20$ and $t\geqq 3m$ with $m\geqq 3$. Here slightly different methods are called for. We recall our formula (*):

$$x_0=\binom{n}{m+t}-\sum_{q=0}^{m-1}\binom{n+q}{m}\binom{t+q-1}{q}.$$

We are going to show that the negative sum is bounded by a certain geometric progression. Consider the ratios of its successive terms:

$$\frac{q\text{-th term}}{(q+1)\text{-st term}}=\binom{n+q}{m}\binom{t+q-1}{q}\Big/\binom{n+q+1}{m}\binom{t+q}{q+1}=\frac{(n+q+1-m)}{(n+q+1)}\cdot\frac{(q+1)}{(q+t)}.$$

This ratio is always less than 1; it is largest when $q=m-2$. In that case the ratio is:

$$\frac{n-1}{n+m-1}\cdot\frac{m-1}{t+m-1}<\frac{m-1}{t+m-1}<\frac{1}{4}\quad\text{as we assume}\quad t\geqq 3m.$$

So all the successive ratios are less than (1/4), and we have:

$$x_0=\binom{n}{m+t}-\sum_{q=0}^{m-1}\binom{n+q}{m}\binom{t+q-1}{t-1}$$
$$>\binom{n}{m+t}-\binom{n+m-1}{m}\binom{t+m-2}{t-1}(1+(1/4)+(1/4)^2+\cdots+(1/4)^{m-1})$$
$$>\binom{n}{m+t}-\tfrac{4}{3}\binom{n+m-1}{m}\binom{t+m-2}{t-1}.$$

I will show that the last expression is greater than zero; we use induction on t— always assuming that (t, k, v) is a putative parameter set with $m=(k-t)\geqq 3$ and $t\geqq 3m$.

First assume that $t=3m$. We must show that:

$$\binom{n}{4m}>\binom{n+m-1}{m}\binom{4m-2}{m-1}\tfrac{4}{3}.$$

Since (t, k, v) is a putative parameter set, its contracted 2-design satisfies Fisher's inequality. Hence

$$\lambda_{t-2,k-t+2}=\binom{n}{m+2}-\sum_{q=0}^{m-1}\binom{n+q}{m}\binom{q+1}{q}\geqq 0.$$

In particular:

$$\binom{n}{m+2}>\binom{n+m-1}{m}m,$$

as this is just the last term of the negative sum.

We now set

$$R^+=\binom{n}{4m}\Big/\binom{n}{m+2}=\frac{(n-m-2)(n-m-3)\dots(n-4m+1)}{(4m)(4m-1)\dots(m+3)}$$

$$R^-=(4/3)\binom{n+m-1}{m}\binom{4m-2}{m-1}\Big/\binom{n+m-1}{m}m=4\cdot\frac{(4m-2)(4m-3)\dots(3m+1)}{(m-1)(m-2)\dots(2)}$$

and notice that if we establish $R^+>R^-$ we will have the inequality proved for $t=3m$. By the strong Fisher's inequality:

$$n-4m+1\geqq m^2-2m+(m+1)^{3/2}+1>m^2 \quad \text{as} \quad m\geqq 3.$$

So all the terms in the numerator of R^+ are greater than m^2. In the denominator, $(m-2)$ terms are $\geqq 2m$, m terms are between $2m$ and $3m$, and m terms are between $3m$ and $4m$. Hence:

$$R^+>\left(\frac{m^2}{2m}\right)^{m-2}\left(\frac{m^2}{3m}\right)^m\left(\frac{m^2}{4m}\right)^m=\left(\frac{m}{2}\right)^{m-2}\left(\frac{m^2}{12}\right)^m.$$

But clearly

$$R^-<4\left(\frac{3m}{2}\right)^{m-2}=\left(\frac{m}{2}\right)^{m-2}\cdot 4\cdot(3)^{m-2}.$$

If $m \geqq 6$ we then have $R^+ > R^-$; if $m = 3, 4$, or 5 we may check our original inequality out by hand. So we have established it for $t = 3m$.

We now finish the proof by using an induction on t, suppose the inequality holds for all parameter sets (t, k, v) with $3m \leqq t < t'$. Now $(t'-1, k-1, v-1)$ is a putative parameter set with the same values of n and m as the set (t', k, v). We have the inequality there, viz.

$$\binom{n}{m+t'-1} > \binom{n+m-1}{m}\binom{t'+m-3}{t'-2}\tfrac{4}{3}.$$

Again we just compare the ratios of the relevant terms:

$$T^+ = \binom{n}{m+t'} \Big/ \binom{n}{m+t'-1} = \frac{v-2k+1}{k}$$

$$T^- = \binom{n+m-1}{m}\binom{t'+m-1}{t'-1}\left(\frac{4}{3}\right) \Big/ \binom{n+m-1}{m}\binom{t'+m-3}{t'-2}\left(\frac{4}{3}\right) = \frac{t'+m-2}{t'-1}.$$

If $T^+ > T^-$ we will have established the inequality for (t', k, v). But as we have $t' \geqq 3m$ and $m \geqq 3$, we have, by Corollary 6 of Theorem 2, that $v \geqq (11/3)k$. Thus $T^+ \geqq (5/3)$. But as $t' \geqq 3m$ we must have $T^- < (5/3)$. This completes the induction and hence the proof of the last case of Theorem 1.

4. Proof of Theorem 2

We begin with a number-theoretic result:

Lemma 9. *If (t, k, v) is a putative parameter set for a Steiner system and we let $S = \{(v-t), (v-t-1), \ldots, (v-k+1)\}$, then no prime or prime power occurring between $(k-t+1)$ and k divides any member of S.*

Proof. Suppose that $(k-t+1) \leqq p^\alpha \leqq k$; by the divisibility conditions we know that

$$\frac{(p^\alpha+v-k)(p^\alpha+v-k-1)\ldots(v-t+1)}{(p^\alpha)(p^\alpha-1)\ldots(k-t+1)} \quad \text{is an integer.}$$

But then I claim p^α must divide one of the terms in the numerator. To see this let p^β be the highest power of p dividing any term in the numerator, and suppose $p^\beta | (p^\alpha+v-k-i)$ where $0 \leqq i \leqq (p^\alpha+t-k-1)$.

The exponent of p dividing the denominator, which we call $p(\text{den.})$, is:

$$\sum_{r=1}^{\alpha-1}\left[\frac{p^\alpha-k+t-1}{p^r}\right]+\alpha.$$

Similarly, the exponent of p dividing the numerator of this expression, $p(\text{num.})$ is precisely:

$$\sum_{r=1}^{\beta}\left[\frac{p^\alpha-k+t-1-i}{p^r}\right]+\left[\frac{i}{p^r}\right]+\beta.$$

But we always have the inequality: $\left[\frac{a}{b}\right] \geqq \left[\frac{a-c}{b}\right] + \left[\frac{c}{b}\right]$. As our quotient is integral, we know that $p(\text{num.}) \geqq p(\text{den.})$. This clearly forces $\beta \geqq \alpha$ and hence $p^\alpha | (p^\alpha + v - k - i)$ with $0 \leqq i \leqq (p^\alpha + t - k - 1)$.

But then p^α does not divide any member of the set

$$\{(p^\alpha + v - k - i - 1), (p^\alpha + v - k - i - 2), \ldots, (v - k - i + 1)\}.$$

Taking the "worst" possible value of i at each end, we still have established that p^α divides no member of S.

We now proceed to the proof of part 1 of Theorem 2. Set $v = 2k + j$ where $j \leqq t + 1$ and put $a = (k - t + 1)$. We assume, to force a contradiction, that $a \geqq 3$.

First we note that $2a \leqq k$. For by the first divisibility conditions we know $a | (v - t + 1) = (k + j + a)$, so $a | (k + j)$. By Fisher's inequality:

$$(v - t + 1) \geqq (k - t + 1)(k - t + 2), \quad \text{or} \quad (k - j) \geqq a^2.$$

As we are assuming that $a \geqq 3$ we either have $k + j \geqq 4a$ or else $a = 3$, $k + j = 9$; as the divisibility conditions fail for $(t, k, v) = (3, 5, 14)$ the latter case does not arise. Hence $4a \leqq k + j \leqq 2k$, as $j \leqq t + 1$, and $2a \leqq k$ as claimed.

We now recall the set $S = \{(v - t), (v - t - 1), \ldots, (v - k + 1)\}$ of the last lemma. Suppose $2r$ is an even element of S, I will show all the prime power factors of $2r$ are less than $a = (k - t + 1)$. For if $p^\alpha | 2r$ and $p^\alpha \geqq a$, then by Lemma 9 we know $p^\alpha > k$. If p is odd this gives:

$$2r \geqq 2p^\alpha \geqq 2(k + 1).$$

However, the largest member of S is $(v - t)$ which is $\leqq (2k + 1)$, a contradiction. The same method works for $p = 2$ except when $2r = 2^\beta$. But as we know $2a \leqq k$ we must have at least one power of 2 between a and k; say 2^γ is the smallest power of 2 greater than a. If $\beta \geqq \gamma$ then $2r$ is divisible by a prime power between a and k, a contradiction. Hence $\beta < \gamma$ and $2^\beta < a$ as claimed.

As we are assuming $a \geqq 3$ the set S has, at the very least, the two members: $(v - t)$, $(v - t - 1)$. One of these must be even. Suppose it is $(v - t)$, then by the previous paragraph all the prime power factors of this number are less than a. Say $p^\alpha | (v - t)$, we know that p^α divides one of the consecutive numbers

$$a, a + 1, \ldots, a + p^\alpha - 1.$$

But as $p^\alpha < a$ we have $a + p^\alpha - 1 < 2a \leqq k$; thus we may use the divisibility conditions to show that if $p^\alpha | a + i$ with $i \leqq p^\alpha - 1$, then

$$\frac{(v - t + i + 1)(v - t + i) \ldots (v - t + 1)}{(a + i)(a + i - 1) \ldots a} \quad \text{is an integer.}$$

By arguments similar to Lemma 9 this implies that p^α divides one of

$$(v - t + i + 1), (v - t + i), \ldots, (v - t + 1)$$

where $i \leqq p^\alpha - 1$. But by assumption $p^\alpha | (v - t)$, so we must have $i = p^\alpha - 1$ and hence $p^\alpha | a + p^\alpha - 1$ or $p^\alpha | a - 1$. As this holds for all prime power factors of $(v - t)$ we must have $(v - t) | (a - 1)$. But then $(v - t) \leqq (a - 1) = (k - t)$ and so $v \leqq k$, a contradiction.

Thus we must have $(v-t)$ odd and hence $(v-t-1)$ even. A similar argument to the above shows then that $(v-t-1)|(a-1)(a-2)$, so we write:

$$m(v-t-1)=m(v-t+1-2)=(a-1)(a-2).$$

By the first divisibility condition, $a|(v-t+1)$. Hence $a|(2m+2)$ and so $a-2\leqq 2m$. But then

$$(v-t+1)=\frac{(a-1)(a-2)}{m}+2\leqq 2(a-1)+2=2a.$$

This contradicts Fisher's inequality and gives us our final contradiction.

To prove part 2 of Theorem 2 we use exactly the same methods, but must deal with a few more exceptional cases along the way. We begin by showing that, with the same notation, $3a\leqq k$ except in the cases $(t,k,v)=(3,6,22)$, $(4,7,23)$, and $(5,8,24)$. We then consider the members of the set S and demonstrate that if $3r$ is a member of S, then all its prime power factors are less than a (This does *not* hold in the exceptional cases). Since we are assuming, to force the contradiction, that $a=k-t+1\geqq 4$, we have at least 3 elements in S: $(v-t)$, $(v-t-1)$, $(v-t-2)$. One must be divisible by 3; if it is $(v-t)$ or $(v-t-1)$ we get a contradiction exactly as we did previously. So we must have $3|(v-t-2)$ and from that it follows that $(v-t-2)|(a-1)(a-2)(a-3)$. We write $m(v-t-2)=(a-1)(a-2)(a-3)$. By the first divisibility condition we know $a|(v-t+1)$, so $a|3(m-2)$. We consider several cases:

I. $m=1$. Then $a|-3$ and $a\leqq 3$ is claimed.

II. $m=2$. Then

$$v-t+1=\frac{a(a^2-6a+11)}{2}.$$

By the first divisibility condition, $(v-t+1)/a$ is an integer, so a must be odd; similarly Fisher's inequality forces $a\geqq 7$. By the *second* divisibility condition:

$$\frac{\left(\frac{a(a^2-6a+11)}{2}+1\right)\cdot\left(\frac{a^2-6a+11}{2}\right)}{(a+1)}\quad \text{is an integer!}$$

This yields $(a+1)|2^5\,3^2$; with all these restrictions we see

$$a\in\{7,11,15,17,23,35,47,71,143,287\}.$$

From these values we may calculate $(v-t+1)$ and test the divisibility conditions for $t\geqq 3$; all cases fail before $v\leqq 4k$ and hence do not satisfy the hypotheses of the Theorem.

III. $m>2$ and so $a\leqq 3(m-2)$.

If $a=3(m-2)$ the second divisibility condition gives us $(a+6)|2^2\,3^2\,7$; Fisher's inequality gives $a\geqq 11$. So $a\in\{12,15,22,30,36,57,78,120,246\}$. Again we may calculate $(v-t+1)$ and notice that in all cases the divisibility conditions fail before $v\leqq 4k$.

If $a=(3/2)(m-2)$ the second divisibility condition yields $(a+3)|120$ and Fisher's implies that $a\geqq 25$. Hence $a\in\{27,37,57,117\}$, none of which yield putative parameter sets satisfying the hypotheses.

So we may safely assume that $a \leqq (m-2)$ and so $(a-1) < m$. But:

$$(v-t-2) = \frac{(a-1)(a-2)(a-3)}{m} < (a-2)(a-3),$$

so $(v-t+1) < a^2$ which contradicts Fisher's inequality and completes the proof of part 2 of the Theorem.

Note. Perhaps this Theorem has a generalization to a result of the form:

$$v \leqq mk + t + (m-1) \quad \text{implies} \quad k \leqq t + (m-1) \quad \text{for all } m$$

with a few (listable) exceptions. Ganter's tables [5] seem to support this conjecture, though there are some violations like (17, 26, 236), where $m = 9$. The method of proof used above shows we get only finitely many exceptions for each value of m, but their number seems to get out of hand.

Acknowledgement. I wish to thank the Marshall Commission for their generous support in the form of a Marshall Scholarship which I held at Oxford University while writing this paper. I also wish to thank my supervisor, Dr. Peter Cameron, for his constant help and encouragement.

References

1. Alltopp, W.O.: An infinite class of 5-designs. J. combinat. Theory, Ser. A **12**, 390–395 (1972)
2. Bruck, R., Ryser, H.J.: The non-existence of certain finite projective planes. Canadian J. Math. **1**, 88–93 (1949)
3. Dembowski, P.: Inversive planes of even order. Bull. Amer. math. Soc. **69**, 850–854 (1963)
4. Dembowski, P.: Möbiusebenen gerader Ordnung. Math. Ann. **157**, 179–205 (1964)
5. Ganter, B.: A Catalogue of Steiner Systems. Darmstadt. Technische Hochschule Darmstadt (1972)
6. Kantor, W.M.: Dimension and embedding theorems for geometric lattices (to appear)
7. Mendelsohn, N.S.: A theorem on Steiner systems. Canadian J. Math. **22**, 1010–1015 (1970)
8. Mendelsohn, N.S., Hung, S.H.Y.: On the Steiner systems $S(3, 4, 14)$ and $S(4, 5, 15)$. Utilitas math. **1**, 5–95 (1972)
9. Noda, R.: Steiner systems which admit block transitive automorphism groups of small rank. Math. Z. **125**, 113–121 (1972)
10. Wilson, R.M., Ray-Chaudhuri, D.K.: Generalization of Fisher's inequality to t-designs. Notices Amer. math. Soc. **18**, 805 (1971)
11. Witt, E.: Über Steinersche Systeme. Abh. math. Sem. Univ. Hamburg **12**, 265–275 (1938)

Benedict H. Gross
Dept. of Mathematics
Harvard University
Cambridge, Mass. 02138
U.S.A.

(Received June 20, 1974)