Can. J. Math., Vol. XXII, No. 5, 1970, pp. 1010–1015

A THEOREM ON STEINER SYSTEMS

N. S. MENDELSOHN

1. Definitions and notation. A generalized Steiner system (t-design, tactical configuration) with parameters t, λ_t, k, v is a system (T, B), where T is a set of v elements, B is a set of blocks each of which is a k-subset of T (but note that blocks b_i and b_j may be the same k-subset of T) and such that every set of t elements of T belongs to exactly λ_t of the blocks. If we put $\lambda_t = u$ we denote by $S_u(t, k, v)$ the collection of all systems with these parameters. Thus $Q \in S_u(t, k, v)$ means $Q = (T, B)$ is a system with the given parameters. If $\lambda_t = u = 1$, we write $S(t, k, v)$ instead of $S_1(t, k, v)$ and refer to the system as a Steiner system. If $t = 2$, the system is called a balanced incomplete block design. If the number of elements equals the number of blocks, we call the system symmetric. Except in the trivial cases, $k = v$ and $k = v - 1$, there are no symmetric systems with $t > 2$ (see [**1**]).

2. Some elementary properties of generalized Steiner systems. We state here without proof some properties of generalized Steiner systems.

(i) If $Q \in S_u(t, k, v)$, where $u = \lambda_t$, then $Q \in S_w(s, k, v)$ where $w = \lambda_s$, $s \leqq t$, and

$$\lambda_s = \lambda_t \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

(ii) The number λ_1 is the number of times any element appears in a block and is often called the replication number. The notation $\lambda_1 = r$ is usually used.

(iii) If $s = 0$, the number λ_0 turns out to be the number of blocks and the notation $\lambda_0 = b$ is usually used.

(iv) From (i), (ii), (iii), the system $S_u(t, k, v)$ has parameters v, k, λ_0, $\lambda_1, \ldots, \lambda_t$. For a symmetric design $v = \lambda_0$ and $k = \lambda_1$.

If $R = (T, B) \in S(t, k, v)$, then

$$Q = (T - \{x\}, B^*) \in S(t-1, k-1, v-1),$$

where x is a fixed element of T and B^* is obtained from B by taking the collection of all blocks of B which contain x and then deleting x from these blocks. In this case we say Q is embedded in R.

Received November 19, 1969.

3. The intersection numbers. Let $Q \in S_u(t, k, v)$. Let b be a fixed block of Q. With respect to the fixed block b we define numbers $x_0, x_1, x_2, \ldots, x_k$ as follows: x_i is the number of blocks distinct from b, each of which has exactly i elements in common with b. In general, the numbers x_i will depend on the block b but as will be seen shortly this will not be so for ordinary Steiner systems $S(t, k, v)$.

In [**1**], the following equations which must be satisfied by a set of intersection numbers were given:

$$
\begin{aligned}
(2)\qquad x_0 + x_1 + \cdots + x_k &= (\lambda_0 - 1)\binom{k}{0}\\
x_1 + 2x_2 + \cdots + kx_k &= (\lambda_1 - 1)\binom{k}{1}\\
&\vdots\\
x_i + \binom{i+1}{i}x_{i+1} + \cdots + \binom{k}{i}x_k &= (\lambda_i - 1)\binom{k}{i}\\
&\vdots\\
x_t + \binom{t+1}{t}x_{t+1} + \cdots + \binom{k}{t}x_k &= (\lambda_t - 1)\binom{k}{t}
\end{aligned}
$$

In the particular case of an ordinary Steiner system, $\lambda_t = 1$, and since the x_i are non-negative integers, $x_t = x_{t+1} = \ldots = x_k = 0$. The system of equations (2) read, in this case, as follows:

$$
\begin{aligned}
(3)\qquad x_0 + x_1 + \cdots + x_t &= (\lambda_0 - 1)\binom{k}{0}\\
x_1 + 2x_2 + \cdots + tx_t &= (\lambda_1 - 1)\binom{k}{1}\\
x_{t-1} + \binom{t}{t-1}x_t &= (\lambda_{t-1} - 1)\binom{k}{t-1}\\
x_t &= 0
\end{aligned}
$$

The equations (3) are t linear equations in t variables and obviously are *uniquely* solvable for $x_0, x_1, \ldots, x_t$.

In particular, we can solve for x_0 in (3) by multiplying the equations alternately by 1 and -1 and adding.

Substituting for the values of λ_i, and manipulating the binomial coefficients yields

$$
(4)\qquad x_0 = \frac{1}{\binom{v-t}{v-k}}\left\{\sum_{i=0}^{t} (-1)^i\binom{k}{i}\binom{v-i}{k-i}\right\} - \sum_{i=0}^{t} (-1)^i\binom{k}{i}.
$$

Equation (4), of course, is only valid for $\lambda_t = 1$, the ordinary Steiner system $S(t, k, v)$.

4. The systems $S(t-1, t, 2t+1)$ and $S(t, t+1, 2t+2)$.

LEMMA 1. *If $S(t-1, t, 2t+1)$ exists, then t is odd.*

Proof. Computing λ_{t-2} we obtain

$$\lambda_{t-2} = \binom{t+3}{1} \Big/ \binom{2}{1} = \frac{t+3}{2}$$

and since λ_{t-2} is an integer, t is odd.

LEMMA 2. *If $S(t-1, t, 2t+1)$ exists, then for any $Q \in S(t-1, t, 2t+1)$ every pair of blocks in Q has a non-null intersection.*

Proof. In equation (4) for x_0, replacing t by $t-1$, and putting $k = t$, $v = 2t+1$, we obtain

$$x_0 = \frac{1}{t+2}\left\{\sum_{i=0}^{t-1} (-1)^i \binom{t}{i}\binom{2t+1-i}{t-i}\right\} - \sum_{i=0}^{t-1} (-1)^i \binom{t}{i}.$$

Replacing i by $t-j$ and using the facts that t is odd and

$$\binom{t}{j} = \binom{t}{t-j},$$

we have

$$x_0 = \frac{1}{t+2}\left\{\sum_{j=1}^{t} (-1)^{j+t} \binom{t}{j}\binom{t+1+j}{j}\right\} + \sum_{j=1}^{t} (-1)^j \binom{t}{j}.$$

Now, using [**2**, p. 9, formula (6)] to reduce the first member of the right side and noting that the second member has the value -1, we obtain

$$x_0 = \frac{1}{t+2}\binom{t+1}{t} + \frac{1}{t+2} - 1 = 0.$$

This implies that every two blocks have a non-null intersection.

LEMMA 3. *Suppose that $S(t, t+1, 2t+2)$ is non-null and that*

$$Q \in S(t, t+1, 2t+2).$$

Then if b is a block of Q, the set $\bar{b}$ which is complementary to b is also a block of Q.

Proof. Since the system Q is based on $2t+2$ elements and its blocks are $(t+1)$-subsets, the sets complementary to blocks are also $(t+1)$-subsets.

If we now apply the same computation as was done in Lemma 2 for this case, we obtain $x_0 = 1$. Hence for every block $b \in Q$ there is exactly one block $\bar{b} \in Q$ which does not intersect it. But the only $(t + 1)$-subset which does not intersect b is the complementary set.

THEOREM 1. *The system* $S(t - 1, t, 2t + 1)$ *is non-null if and only if the system* $S(t, t + 1, 2t + 2)$ *is non-null. If* $Q \in S(t - 1, t, 2t + 1)$, *there exists exactly one system* $R \in S(t, t + 1, 2t + 2)$ *in which* Q *is embedded.*

Proof. Suppose that $S(t, t + 1, 2t + 2)$ is non-null. Then if

$$R \in S(t, t + 1, 2t + 2),$$

the blocks of R which contain a fixed element x determine a

$$Q \in S(t - 1, t, 2t + 1)$$

where the blocks of Q are obtained by deleting x from the above set of blocks.

Now suppose that $S(t - 1, t, 2t + 1)$ is non-null and let

$$Q = (T, B) \in S(t - 1, t, 2t + 1).$$

Let $T = \{1, 2, \ldots, 2t + 1\}$ and $B = \{b_1, b_2, \ldots, b_{\lambda_0}\}$. A direct calculation of λ_0 in each case shows that if

$$Q \in S(t - 1, t, 2t + 1) \qquad \text{and} \qquad R \in S(t, t + 1, 2t + 2),$$

then R must have exactly twice as many blocks as Q. Define $R = (T^*, B^*)$, where

$$T^* = \{1, 2, 3, \ldots, 2t + 1, 2t + 2\}$$

and

$$B^* = \{b_1^*, b_2^*, \ldots, b_{\lambda_0}^*, \bar{b}_1^*, \bar{b}_2^*, \ldots, \bar{b}_{\lambda_0}^*\},$$

where $b_i^* = b_i \cup \{2t + 2\}$ and $\bar{b}_i^* = T^* - b_i^*$ for $i = 1, 2, \ldots, \lambda_0$. We show that $R \in S(t, t + 1, 2t + 2)$. First note that the number of t-tuples which can be obtained from the blocks of B^* is exactly the number of t-tuples which can be formed from the elements of T^*. Hence it is sufficient to show that no t-tuple appears in two different blocks of B^*. We distinguish three cases.

Case 1. b_i^* and b_j^* have a common t-tuple. In this case when the element $2t + 2$ is deleted from b_i^* and b_j^* the elements b_i and b_j would have a common $(t - 1)$-tuple which contradicts the fact that $Q \in S(t - 1, t, 2t + 1)$.

Case 2. $\bar{b}_i^*$ and $\bar{b}_j^*$ have a common t-tuple, say $\{1, 2, 3, \ldots, t\}$. Then $\bar{b}_i^* = \{1, 2, 3, \ldots, t, v\}$ and $\bar{b}_j^* = \{1, 2, 3, \ldots, t, w\}$. Then

$$b_i = \{t + 1, t + 2, \ldots, 2t + 2\} - \{v\}$$

and $b_j = \{t + 1, t + 2, \ldots, 2t + 2\} - \{w\}$ have a common t-tuple which reduces to Case 1.

Case 3. b_i^* and $\bar{b}_j^*$ have a common t-tuple. In this case we may take b_i^* to be $\{1, 2, \ldots, t, 2t+2\}$ and $\bar{b}_j^* = \{1, 2, 3, \ldots, t, v\}$, where $t+1 \leqq v \leqq 2t+1$; then $b_j^* = \{t+1, t+2, \ldots, v-1, v+1, \ldots, 2t+1\}$. Hence $b_i = \{1, 2, \ldots, t\}$ and $b_j = \{t+1, t+2, \ldots, v-1, v+1, \ldots, 2t+1\}$. Hence b_i and b_j are two non-intersecting blocks of Q. By Lemma 2, this yields a contradiction. The fact that the embedding of Q in R is unique follows from Lemma 3 and from the fact that R has exactly twice as many blocks as Q.

5. Examples and extension. Actual examples of Theorem 1 are the embedding of $S(2, 3, 7)$ in $S(3, 4, 8)$ and of $S(4, 5, 11)$ in $S(5, 6, 12)$, the latter systems being associated with the Mathieu groups M_{11} and M_{12}. The next possible case would be an embedding of $S(8, 9, 19)$ in $S(9, 10, 20)$ if either of these designs exist.

Suppose now we consider the generalized Steiner system $S_u(t, k, v)$ with $u = \lambda_t$. Equations (2) no longer need have a unique solution. However, if we restrict ourselves to generalized Steiner systems in which no two blocks intersect in more than t points it is true that equations (2) have a unique solution and we can proceed as before.

LEMMA 4. *Suppose that* $Q \in S_u(t, k, v)$ *and that no two blocks of* Q *intersect in more than* t *points. Then*

$$x_0 = \frac{u}{\binom{v-t}{v-k}} \left\{ \sum_{i=0}^{t} (-1)^i \binom{k}{i} \binom{v-i}{k-i} \right\} - \sum_{i=0}^{t} (-1)^i \binom{k}{i}. \tag{5}$$

Proof. Same as that for equation (4).

LEMMA 5. *If* $Q \in S_u(t-1, t, 2t+1)$ *and* Q *has no repeated blocks, then* $x_0 = u - 1$.

Proof. Substitute into equation (5) and simplify.

LEMMA 6. *If* $R \in S_u(t, t+1, 2t+2)$ *and* R *has no repeated blocks, then* $x_0 = 1$.

Proof. Substitute into equations (5) and simplify.

THEOREM 2. *The system* $S_u(t-1, t, 2t+1)$ *contains designs without repeated blocks if and only if the system* $S_u(t, t+1, 2t+2)$ *contains designs without repeated blocks. Any such* $Q \in S_u(t-1, t, 2t+1)$ *is uniquely embeddable in an* $R \in S_u(t, t+1, 2t+2)$ *as follows. Adjoin a new symbol to each of the blocks of* Q *and then the design* R *consists of the augmented blocks and their complements.*

Proof. Use the results of Lemmas 5 and 6 and argue along lines similar to those used in Theorem 1.

The following example illustrates Theorem 2. In $S_2(2, 3, 7)$ there exists the system Q whose blocks are:

1	2	4
2	3	5
3	4	6
4	5	7
5	6	1
6	7	2
7	1	3
1	2	6
2	3	7
3	4	1
4	5	2
5	6	3
6	7	4
7	1	5

Note here that by Lemma 5 each block has exactly one other block which does not intersect it; e.g., 1 2 4 and 5 6 3. Then Q is embedded in $R \in S_2(3, 4, 8)$ as follows:

1	2	4	8		3	5	6	7
2	3	5	8		1	4	6	7
3	4	6	8		1	2	5	7
4	5	7	8		1	2	3	6
5	6	1	8		2	3	4	7
6	7	2	8		1	3	4	5
7	1	3	8		2	4	5	6
1	2	6	8		3	4	5	7
2	3	7	8		1	4	5	6
3	4	1	8		2	5	6	7
4	5	2	8		1	3	6	7
5	6	3	8		1	2	4	7
6	7	4	8		1	2	3	5
7	1	5	8		2	3	4	6

An examination of this example shows how the argument in Theorem 1 should be modified to obtain Theorem 2.

REFERENCES

1. N. S. Mendelsohn, *Intersection numbers of t-designs*, Notices Amer. Math. Soc. *16* (1969), 984. (Also University of Manitoba mimeographed series.)

2. J. Riordan, *Combinatorial identities* (Wiley, New York, 1968).

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

The University of Manitoba,
Winnipeg, Manitoba