ON STEINER SYSTEM S(5, 8, 24) AND THE MIRACLE OCTAD GENERATOR (MOG)

SITT CHEE KEEN

UNIVERSITI SAINS MALAYSIA

2004

ON STEINER SYSTEM S(5, 8, 24) AND THE MIRACLE OCTAD GENERATOR (MOG)

by

SITT CHEE KEEN

Thesis submitted in fulfillment of the

requirements for the degree

of Master of Science

August 2004

ACKNOWLEDGEMENTS

First of all, I would like to express my gratitude to my supervisor Dr. Hajar Sulaiman who direct my interest towards the study of combinatorial structure. She has given me lots of support, and willing to struggle with me in solving problems during the writing of this thesis. I am also grateful to Associate Professor How Guan Aun for his encouragement and concern.

I would like to thank University Science of Malaysia that has made it possible for me to pursue my master degree through the sponsorship under the Graduate Assistant Scheme (Skim Siswazah Pembantu).

I will never forget my fellow post-graduate Mr. Dasmen Teh Wen Chean for his companionship. Never forget Associate Professor Ong Boon Hua, Dr. Andrew Rajah, Dr. Hailiza, En. Adam, En. Helmi Samsudin, Pn. Faridah, all faculty members and staff of the School of Mathematical Sciences.

Finally, this thesis is dedicated to my parents and my grandmother with love and much appreciation.

TABLE OF CONTENTS

PAGE NUMBER

INDEX OF NOTATION

$\Rightarrow$	implies that
$\{ x \mid P(x) \}$	set of all elements x that satisfy the condition $P(x)$
$\in$	belongs to
$\notin$	not belongs to
$=$	equals to
$\neq$	not equals to
$A \subset B$	A is a subset of B
$A \not\subset B$	A is not a subset of B
$A \cap B$	intersection of A and B
$A \cup B$	union of A and B
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	2×2 matrix
$a \leq b$	a is less than or equals to b
$a < b$	a is strictly less than b
Z_2	cyclic group of order 2
$\binom{n}{r}$	combination of r items from n items
S(l, m, n)	Steiner system
$E_{i,j}$	number of octads containing j elements out of i elements
P(Ω)	power set of set Ω
1 – 1	one to one correspondence
X'	compliment of set X
$\lvert X \rvert$	number of elements in set X

$A \setminus B$	the set of points in A but not in B
$\mathbf{C}$	space $\mathbf{C}$
$\mathbf{C}$-sets	elements in space $\mathbf{C}$
$n!$	n factorial
Λ_i	heavy brick i
$\Re^n$	n – dimensional real space

SISTEM STEINER S(5, 8, 24) DAN

PENJANA OKTAD AJAIB

ABSTRAK

Sistem Steiner S(*l, m, n*) terdiri daripada subset –subset *m* unsur bagi set *n* unsur Ω di mana setiap subset *l* unsur bagi set *n* unsur terkandung dalam hanya satu subset *m* unsur. Sistem Steiner yang paling menarik perhatian ialah sistem Steiner yang mempunyai nilai *l* yang sebesar mungkin. Tetapi hingga sekarang, hanya terdapat dua sahaja sistem Steiner di mana $l > 4$ yang diketahui. Salah suatu daripada meraka ialah S(5, 8, 24).

Matlamat utama tesis ini adalah untuk memperlihatkan hubungan antara Penjana Oktad Ajaib (Miracle Octad Genarator) dengan sistem Steiner S(5, 8, 24). Pada permulaannya, kami membuktikan kewujudan sistem Steiner S(5, 8, 24). Seterusnya, kami membuktikan keunikan sistem Steiner ini selepas melabel semula titik-titik dalam set yang mengandungi 24 unsur Ω. Selanjutnya kami tunjukkan bahawa Penjana Oktad Ajaib dapat memberi kami semua unsur dalam sistem Steiner S(5, 8, 24). Semua bahan yang diperlui telah dimasukan dalam tesis ini. Perspektif tesis ini adalah secara kombinatorik tulen.

ABSTRACT

A Steiner system S*(l, m, n)* is a collection of *m*-element subsets of an *n*-element set Ω such that every *l*-element subset of Ω lies in exactly one of the *m*-element sets. The most interesting Steiner systems are those with *l* as large as possible. But only two systems are known with $l > 4$. One of them is S(5, 8, 24).

The main objective of this thesis is to show the relevance of the Miracle Octad Generator (MOG) with Steiner system S(5, 8, 24). First we show the existence of Steiner system S(5, 8, 24). Next we show that Steiner system S(5, 8, 24) is unique up to relabelling the points of the 24-element set Ω. Then we show that S(5, 8, 24) is given by the Miracle Octad Generator. The treatment in this thesis is self – contained and purely combinatorial.

CHAPTER 1 - INTRODUCTION

In 1853, the Swiss geometer J. Steiner posed the following question:

" Given an N-element set such that every 2-element subset of N-element set lies in exactly one 3-element subset of N-element set. Does this kind of N-element set exist ? " If we write l, m and n instead of 2, 3 and N, respectively, then we have the following combinatorial structure that we called the Steiner system : A *Steiner system* S(l, m, n) is a finite set Ω of elements (called *points*) with a family of subsets (called *blocks*) such that the following holds true:

1. There are exactly n points in Ω.
2. Each block has exactly m points.
3. Any l distinct points belong to a unique block.

In order to avoid trivialities it is usually assumed that $2 \le l < m < n$. So Steiner asked for S(2, 3, n) systems. As a matter of fact, T.P.Kirkman proved already in 1847 that a Steiner system S(2, 3, n) exist if and only if $n \equiv 1, 3 \pmod 6$ (see [17]).

Let X be a v-set (i.e.a set with v elements) whose elements are called points. A t-design is a collection of distinct k-subsets (called blocks) of X with the property that any t-subset of X is contained in exactly λ blocks. This is also called a t-(v, k, λ) design. If $\lambda = 1$, a t-design is called a S(t, k, v) Steiner system. In our case, we use l, m and n instead of t, k and v.

There are only two Steiner systems when $l = 5$. One of them is S(5, 6, 12) which is also called *small Witt design* W_{12}. It was firstly presented by E. Witt in his paper *Uber Steinersche Systeme* in 1938. Another Steiner system is S(5, 8, 24) which is also called *large Witt design* W_{24}. It was due to R.D.Carmichael (see [5]). Historically, the construction problems of designs was first handled by statisticians, since designs with the right parameters were needed in the design of experiments (see [20]).

A remarkable property of the two Steiner systems concerns their automorphism groups. The automorphism groups of S(5, 6, 12) and S(5, 8, 24) act 5-transitively on their sets of points. These automorphism groups are the *Mathieu groups* M_{12} and M_{24}, respectively. These two quintuply transitive permutation groups which act on twelve and twenty-four points respectively were discovered by the French mathematician Emil Mathieu in 1861 in his paper *Memoire sur l'etude des functions de plusieurs quantites* and 1873 in his another paper *Sur la function cinq fois transitive de 24 quantites.*

M_{12} and M_{24} are early examples of *sporadic finite simple groups*. Simple groups may be viewed as the atoms of finite group theory. In one of the most remarkable achievements of human endeavor, the complete list of the finite simple groups was obtained in the early 1980s. Gorenstein estimates that the full details of the classification occupy about 15,000 pages in research journals and that this work involved about 400 research mathematicians from many different countries. A deeper account of the classification can be obtained by consulting the book by Gorenstein (see [16]) or the book by Aschbacher (see [2]).

With the classification of finite groups complete, we now know that any other quintuply transitive permutation group, on any number of points, must contain the corresponding alternating group. Indeed, the only quintuply transitive groups, other than the alternating and symmetric groups, are in the point stabilizers in M_{12} and M_{24}, which are denoted by M_{11} and M_{23} respectively. To put it another way, the study of multiply (≥ 4 fold) transitive groups now means the study of the symmetric groups and the Mathieu groups (see [13]).

Apart from their beauty and interest in their own right, the Mathieu groups are involved in many of the other sporadic simple groups (see [8]). Thus a detailed understanding of the other exceptional groups necessitates an intimate knowledge of M_{12} and M_{24}. Since M_{12} and M_{24} are automorphism groups of S(5, 6, 12) and S(5,8,24) respectively, those two Steiner systems are indeed remarkable combinatorial structures. For many decades, S(5, 6, 12) and S(5, 8, 24) were the only known Steiner systems with parameter $l = 5$. Until recently only finitely many Steiner system S(l, m, n) with $l > 3$ and none with $l > 5$ seem to be known (see [3], [7], [19]).

The Miracle Octad Generator (MOG) is a device invented by Robert Curtis (see [12]) for computing with the elements (called *octads*) of the Steiner system S(5, 8, 24) and the permutations of the Mathieu group M_{24}. Usually, when one constructs a large group from some "simpler" object, the construction itself will have a smaller group of symmetries. And one finds that elements inside this "visible subgroup" are "easy" to understand and the others "hard". It is a remarkable fact that the MOG construction manages to have several "visible groups", each of them a maximal subgroup of M_{24}. Chang Choi discussed the maximal subgroups of M_{24} without using the MOG in 1972

(see [6]). In the same year, Curtis discussed the maximal subgroups of M_{24} by using the MOG (see [15]). So it is always convenient to use MOG arrangement for vectors in $\Re^{24}$ (see also [9], [10]). This indicates that MOG is a device which has theoretical as well as practical value.

Combinatorics is generally concerned with counting arrangements within a finite set. One of the basic problems is to determine the number of possible configurations of a given kind. Even when the rules specifying the configuration are relatively simple, the questions of existence and enumeration often present great difficulties. Besides counting, combinatorics is also concerned with questions involving morphisms and uniqueness of these arrangements.

The main objective of this thesis is to show the relevance of the Miracle Octad Generator (MOG) with Steiner system S(5, 8, 24). First we show the existence of S(5, 8, 24). Next we show that S(5, 8, 24) is unique up to relabelling the points of the 24-element set Ω. Then we show that S(5, 8, 24) is given by the Miracle Octad Generator. The treatment in this thesis is self – contained and purely combinatorial. Throughout the study of this subject, we refer to [12].

Here we list our two main results.

(1) **Corollary 4.4.1′** Corresponding to each four points of Ω, there is a unique partition of the twenty-four points into six tetrads with the property that the union of any two tetrads is an octad. Such a configuration is called a *sextet.*

(2) Section 4.5 – Using the MOG to find sextet defined by a tetrad.

At this stage, we discuss the organization of the chapters in this thesis. The material is divided into five chapters. An introduction to the topics we are going to discuss is given in Chapter 1. Chapter 2 serves as the prerequisites for Chapter 3. Some properties of vector spaces and Steiner systems S(*l, m, n*) are stated in Chapter 2. Chapter 3 is devoted to the construction and existence of S(5, 8, 24). Included in this chapter is the Leech Table. There are five sections in Chapter 4. Miracle Octad Generator (MOG) is discussed in the first section of Chapter 4. Second section contains examples showing how to complete an octad of S(5, 8, 24) from any five given points. In the third section of Chapter 4, we discuss about intersection of octads. A special configuration called *sextet* is discussed in the fourth section. The method of how to use MOG to find sextet defined by a tetrad is included in the last section of Chapter 4. The theme developed in Chapter 4 is then used in Chapter 5 to show the uniqueness of S(5,8,24) up to isomorphism.

CHAPTER 2 - PREREQUISITES

In section 2.1, we list out all properties of vector spaces that we need. In the later part of section 2.1, we talk about power set and symmetric difference. Then in section 2.2, we define Steiner system S(*l, m, n*) and derive some basic facts concerning S(*l, m, n*). Most of the materials in this chapter serve as prerequisites for proving the existence of S(5, 8, 24) in chapter 3. Throughout section 2.1, we follow the treatment in [18]. While in section 2.2, we refer to [1].

2.1 Vector spaces

First we give the definition of vector space over field *K*.

Definition 2.1.1 Let *K* be a given *field* and let *V* be a non-empty set with rules of addition and scalar multiplication which assigns to any $u, v \in V$ a *sum* $u + v \in V$ and to any $u \in V, k \in K$ a *product* $ku \in V$. Then *V* is called a *vector space over K* (and the elements of *V* are called vectors) if the following axioms hold:

A1. For any vectors $u, v, w \in V$, $(u + v) + w = u + (v + w)$.

A2. There is a vector in *V*, denoted by *0* and called the *zero vector*, for which $u + 0 = u$ for any vector $u \in V$.

A3. For each vector $u \in V$, there is a vector in *V*, denoted by $-u$, for which $u + (-u) = 0$.

A4. For any vectors $u, v \in V$, $u + v = v + u$.

M1. For each scalar $k \in K$ and any vectors $u, v \in V$, $k(u + v) = ku + kv$.

M2. For any scalar $a, b \in K$ and any vector $u \in V$, $(a + b)u = au + bu$.

M3. For any scalar $a, b \in K$ and any vector $u \in V$, $(ab)u = a(bu)$.

M4. For $1 \in K$, $1u = u$ for any vector $u \in V$.

The above axioms naturally split into two sets. The first four are only concerned with the additive structure of V. It follows that any sum of vectors of the form $v_1 + v_2 + \cdots + v_m$ requires no parenthesis and does not depend upon the order of the sum, the zero vector 0 is unique, the *negative* $-u$ of each u is unique, and the cancellation law holds. Also subtraction is defined by $u - v = u + (-v)$. On the other hand, the remaining four axioms are concerned with the "action" of the field K on V.

Let W be a subset of a vector space V over a field K. W is called a subspace of V if W is itself a vector space over K with respect to the operations of vector addition and scalar multiplication of V. Simple criteria for identifying subspaces follow.

Theorem 2.1.2 W is a subspace of V if and only if

(i) W is nonempty,

(ii) W is closed under vector addition: $v, w \in W$ implies $v + w \in W$,

(iii) W is closed under scalar multiplication: $v \in W$ implies $kv \in W$ for all $k \in K$.

Proof. See [18] Theorem 4.2.

Corollary 2.1.3 W is a subspace of V if and only if (i) $0 \in W$, and (ii) $v, w \in W$ implies that $av + bw \in W$ for every $a, b \in K$.

Proof. See [18] Corollary 4.3.

Let V be a vector space over a field K and let $v_1, \cdots, v_m \in V$. Any vector in V of the form $a_1v_1 + a_2v_2 + \cdots + a_mv_m$ where the $a_i \in K$, is called a linear combination of $v_1, \cdots, v_m$. The following theorem applies.

Theorem 2.1.4 Let S be a nonempty subset of V. The set of all linear combinations of vectors in S, denoted by $L(S)$, is a subspace of V containing S. Furthermore, if W is any other subspace of V containing S, then $L(S) \subset W$.

Proof. See [18] Theorem 4.5.

In other word, $L(S)$ is the smallest subspace of V containing S ; hence it is called the subspace spanned or generated by S. For convenience, we define $L(\phi) = \{0\}$.

Let U and W be subspaces of a vector space V. The sum of U and W, written $U+W$, consists of all sums $u + w$ where $u \in U$ and $w \in W$:

$$U + W = \{ u + w \mid u \in U, w \in W\}.$$

Note that $0 = 0 + 0 \in U + W$, since $0 \in U$, $0 \in W$. Furthermore, suppose $u + w$ and $u' + w'$ belong to $U + W$ with $u, u' \in U$ and $w, w' \in W$. Then

$$(u + w) + (u' + w') = (u + u') + (w + w') \in U + W.$$

And for any scalar k, $k(u + w) = ku + kw \in U + W$.

Thus we have proven the following theorem.

Theorem 2.1.5 The sum $U + W$ of the subspaces U and W of V is also a subspace of V.

Let U and W be subspaces of a vector space V. And let $\{u_i\}$ generates U and $\{w_j\}$ generates W where $i, j \in \mathbb{Z}^+$. What is the vector space generated by $\{u_i, w_j\}$? We have the answer in the following theorem.

Theorem 2.1.6 Suppose U and W are subspaces of a vector space V, and that $\{u_i\}$ generates U and $\{w_j\}$ generates W. Then $\{u_i, w_j\}$ generates $U+W$.

Proof. See [18] Solved problem 4.35.

Definition 2.1.7 The vector space V is said to be the *direct sum* of its subspaces U and W, denoted by $V = U \oplus W$ if every vector $v \in V$ can be written in one and only one way as $v = u + w$ where $u \in U$ and $w \in W$.

The following theorem applies.

Theorem 2.1.8 The vector space V is the direct sum of its subspaces U and W if and only if (i) $V = U + W$ and (ii) $U \cap W = \{0\}$.

Proof. See [18] Theorem 4.9.

Now we discuss a bit about basis and dimension. We begin with a definition.

Definition 2.1.9 A vector space V is said to be of *finite dimension n* or to be *n-dimensional*, written dim $V = n$, if there exist linearly independent vectors

$A_1, A_2, \cdots, A_n$ which span V. The set $\{ A_1, A_2, \cdots, A_n \}$ is called a *basis* of V.

The above definition of dimension is well defined in view of the following theorem.

Theorem 2.1.10 Let V be finite dimensional vector space. Then every basis of V has the same number of elements.

Proof. See [18] Theorem 5.3.

The vector space $\{0\}$ is defined to have dimension 0. (In certain sense this agree with the above definition since, by definition, ϕ is independent and generates $\{0\}$.) When a vector space is not of finite dimensional, it is said to be of *infinite dimension.* The following theorems give basic relationship between the dimension of a vector space and the dimension of a subspace.

Theorem 2.1.11 Let W be a subspace of an n – dimensional vector space V. Then $\dim W \leq n$. In particular if $\dim W = n$, then $W = V$.

Proof. See [18] Theorem 5.7.

Theorem 2.1.12 Let U and W be finite – dimensional subspaces of a vector space V. Then $U + W$ has finite dimension and

$$\dim (U + W) = \dim U + \dim W - \dim (U \cap W).$$

Proof. See [18] theorem 5.8.

Now suppose V is the direct sum of U and W, i.e. $V = U \oplus W$, then the following theorem applies.

Theorem 2.1.13 Suppose V is the direct sum of its subspaces U and W, i.e. $V=U \oplus W$. Then dim V = dim U + dim W.

Proof. See [18] Solved problem 5.48.

For a finite set Ω, subsets of Ω which contain even number of elements are called *even subsets* of Ω. Otherwise they are called *odd subsets* of Ω. The following theorems are about the number of elements of a *power set* $P(\Omega)$, and the relationship between even subsets and odd subsets of Ω. Power set $P(\Omega)$ is the set that contains all the subsets of Ω.

Theorem 2.1.14 Let Ω be a set with n elements. Then the power set of Ω, $P(\Omega)$, contains 2^n elements.

Proof. See [1] section 2.5(9).

Theorem 2.1.15 Let Ω be a finite set. The number of even subsets of Ω is same as the number of odd subsets of Ω.

Proof. Refer to the proof of Theorem 2.1.14.

At this point, we pay attention to the idea of *symmetric difference*. If A and B are two subsets of a set S, the symmetric difference, $A + B$, is defined to be the set of all elements of S which are in A or B but not both. $A + B$ is shaded as shown in Figure 2.1.1.

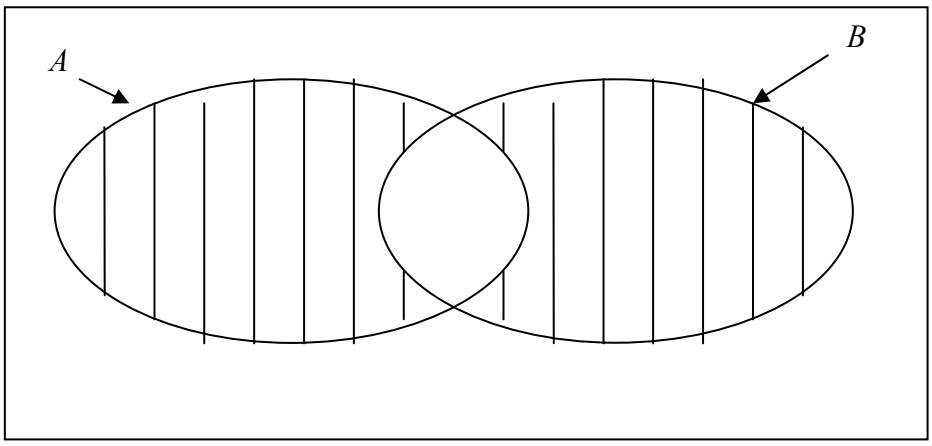


Figure 2.1.1

Let A, B, C be subsets of set S. Clearly it is always true that $A + B = B + A$. And the following are also easily verified : $A + A = \phi$ (the empty set) ; $A + \phi = A$; $A + (B + C) = (A + B) + C$. We have the following theorem after checking all the axioms in Definition 2.1.1.

Theorem 2.1.16 The power set of Ω, $\mathrm{P}(\Omega)$, is a vector space over field Z_2 under addition defined as symmetric difference and scalar multiplication defined as

$$\alpha \cdot x = \begin{cases} x, & \alpha = 1 \\ \phi, & \alpha = 0 \end{cases} \quad \text{where } \alpha \in Z_2, x \in \mathrm{P}(\Omega).$$

2.2 Steiner System S(*l, m, n*)

We start with the definition of Steiner system S(*l, m, n*).

Definition 2.2.1 A *Steiner system S(l, m, n)* is a collection of *m*-element subsets of an *n*-element set Ω such that every *l*-element subset of Ω lies in exactly one of the *m*-element sets. The set Ω is called the *base set*.

The number of elements (*m* – element sets) of S(*l, m, n*) if it exist is given in the following theorem.

Theorem 2.2.2 The number of *m*-element sets in S(*l, m, n*) is $\binom{n}{l} \Big/ \binom{m}{l}$.

Proof. There are $\binom{n}{l}$ *l*-element sets of *n*-element set Ω. Each *l*-element set lies in exactly one of the *m*-element sets. And each *m*-element set contains $\binom{m}{l}$ *l*-element sets.

So $\binom{n}{l}$ = (number of *m*-element sets) $\binom{m}{l}$.

Q.E.D.

Theorem 2.2.2 implies that if a Steiner system S(*l, m, n*) exist, $\binom{n}{l} \Big/ \binom{m}{l}$ must be an integer. But if $\binom{n}{l} \Big/ \binom{m}{l}$ is an integer, it does not necessary implies that S(*l, m, n*) exist. Let us look at some examples.

Example 2.2.1 There does not exist a system S(5, 7, 13)since $\binom{13}{5} \Big/ \binom{7}{5}$ is not an integer.

At this point, an interesting question is, if a Steiner system S(*l, m, n*) exist, can we find 'smaller' Steiner system from S(*l, m, n*) after removing some elements from base set and those *m*-element sets of S(*l, m, n*) containing them? The answer is given in the following theorem.

Theorem 2.2.3 Let *x* be an element of the base set Ω of S(*l, m, n*). The *m*-element sets of S(*l, m, n*) containing *x*, on the removal of *x*, form a Steiner system S(*l*-1, *m*-1, *n*-1).

Proof. If *x* is removed from those *m*-element sets of S(*l, m, n*) and the base set Ω, we have *m*-1 elements left in those *m*-element sets which contain *x*. And the number of elements in base set now become *n*-1. Thus a collection of (*m*-1)-element subsets of an (*n*-1)-element set is obtained. But does each (*l*-1)-element subset lies in exactly one of the (*m*-1)-element set? Assume that an (*l*-1)-element set lies in two different (*m*-1)-element sets. Each (*l*-1)-element subsets, after adding back the *x*, is in a unique *m*-element set. If the assumption is true, then the (*l*-1)-element set, after adding *x*, lies in two different *m*-element sets. This contradict with the definition of S(*l, m, n*). Thus each (*l*-1)-element subset lies in a unique (*m*-1)-element set. Hence a system S(*l*-1, *m*-1, *n*-1) is obtained.

Q.E.D.

Corollary 2.2.4 If a Steiner system S(*l, m, n*) exist, the number of *m*-element sets containing an element of *n*-element set is given by $\binom{n-1}{l-1} \Big/ \binom{m-1}{l-1}$.

Proof. From Theorem 2.2.3, those *m*-element sets containing a particular element *x* of the base set, on the removal of *x*, form a Steiner system S(*l*-1, *m*-1, *n*-1). From Theorem 2.2.2, the number of (*m*-1)-element sets in S(*l*-1, *m*-1, *n*-1) is $\binom{n-1}{l-1} \Big/ \binom{m-1}{l-1}$, which is same as the number of *m*-element sets containing *x*.

Q.E.D.

The generalization of the above theorem is to consider the Steiner system after the removal of *u* elements where $u < l$. We have the following theorem.

Theorem 2.2.5 If a Steiner system S(*l, m, n*) exist, so does a Steiner system S(*l-u, m-u, n-u*) for each $u < l$.

Proof. From Theorem 2.2.3, if a Steiner system S(*l, m, n*) exist, so does a Steiner system S(*l*-1, *m*-1, *n*-1). The (*m*-1)-element sets of S(*l*-1, *m*-1, *n*-1) containing an element *y*, on the removal of *y*, form a Steiner system S(*l*-2, *m*-2, *n*-2). By applying the same procedure, the result follows.

Q.E.D.

Theorem 2.2.5 gives more conditions on *l, m, n* since not only $\binom{n}{l}\Big/\binom{m}{l}$ must be an integer, but so must $\binom{n-1}{l-1}\Big/\binom{m-1}{l-1}, \binom{n-2}{l-2}\Big/\binom{m-2}{l-2}, \ \cdots \ ,$ $\binom{n-(l-1)}{1}\Big/\binom{m-(l-1)}{1}$.

Example 2.2.2 S(5, 8, 24) is a Steiner system. So does S(4, 7, 23), S(3, 6, 22), S(2, 5, 21) and S(1, 4, 20).

Example 2.2.3 An S(2, $n+1$, n^2+n+1) Steiner system is called a *projective plane* of order *n*. Now let us investigate this kind of Steiner system where $n = 6$. Theorem 2.2.5 does not exclude the possibility of the existence of S(2, 7, 43), since $\binom{43}{2}\Big/\binom{7}{2}$ and $\binom{42}{1}\Big/\binom{6}{1}$ are integers. However such a system does not exist. If Steiner system S(2, 7, 43) exist, any S(2, 7, 43) would be a finite projective plane of order 6. But there is no finite projective plane of order 6 (see [1] Theorem 6.4).

At last we have the following corollary as the consequence of Theorem 2.2.5.

Corollary 2.2.6 If a Steiner system S(*l, m, n*) exist, the number of *m*-element sets containing certain *u* elements of *n*-element set where $u < l$ is given by $\binom{n-u}{l-u}\Big/\binom{m-u}{l-u}$.

Proof. From Theorem 2.2.5, if a Steiner system S(*l, m, n*) exist, we know that S(*l-u, m-u, n-u*) exist. And the number of (*m-u*)-element sets in S(*l-u, m-u, n-u*) which is $\binom{n-u}{l-u} \Big/ \binom{m-u}{l-u}$, is also same as the number of *m*-element sets of S(*l, m, n*) containing certain *u* elements of *n*-element set.

Q.E.D.

CHAPTER 3 - EXISTENCE OF S(5, 8, 24)

A Steiner system S(5, 8, 24) is a collection of 8-element subsets (called *octads*) of a 24-element set, Ω, with the property that any 5 elements of the 24 elements lie in a unique octad. In Section 3.1, a special table called Leech Table is introduced. For a particular octad, entry $E_{i,j}$ from the table will give us the number of octads in S(5, 8, 24) containing j elements out of i elements from that fixed octad. Section 3.2 is devoted to the construction and existence of Steiner system S(5, 8, 24). Throughout Section 3.1 and Section 3.2, we follow the treatment in [12].

3.1 Introduction

From Theorem 2.2.2, the number of octads in S(5, 8, 24) is 759 ($=\binom{24}{5}\Big/\binom{8}{5}$).

According to Corollary 2.2.4, each element of Ω lies in 253 ($=\binom{23}{4}\Big/\binom{7}{4}$) octads.

For each case of a given u-element subset of Ω where $2 \le u \le 4$, the number of octads containing certain u elements of Ω is obtained by applying Corollary 2.2.6. Meanwhile each 5-element subset of Ω or *quintuple* lies in exactly one octad. Thus we have the following results.

Theorem 3.1.1 Let Ω be a 24-element set. In S(5, 8, 24),

(a) the number of octads is 759,

(b) each element of Ω lies in 253 octads,

(c) each pair of elements lies in 77 octads,

(d) each triple of elements lies in 21 octads,

(e) each 4-element subsets of Ω (*tetrad*) lies in 5 octads,

(f) each 5-element subsets of Ω (*quintuple*) lies in a unique octad.

Now we are going to introduce a table called Leech Table.

Table 3.1.1 (Leech Table)

Line(*i*)	0	1	2	3	4	5	6	7	8
0	759								
1	506	253							
2	330	176	77						
3	210	120	56	21					
4	130	80	40	16	5				
5	78	52	28	12	4	1			
6	46	32	20	8	4	0	1		
7	30	16	16	4	4	0	0	1	
8	30	0	16	0	4	0	0	0	1
	0	1	2	3	4	5	6	7	8

Entry(*j*)

Fix a particular octad. Let the *j*-th entry at the *i*-th line, $E_{i,j}$, denote the number of octads in the S(5, 8, 24) containing *j* particular elements out of certain *i* elements from the fixed octad where $j \le i$. For example, $E_{2,2} = 77$ and $E_{6,3} = 8$.

From Theorem 3.1.1(b), we know that among all 759 octads, there are 253(= $E_{1,1}$) octads containing a given element of Ω. And there are 759 – 253 = 506($E_{1,0}$) octads which do not contain that given element. 77(= $E_{2,2}$) octads contain a given 2-element subset of Ω. Let *x, y* be any two elements. Among those 253 octads containing *x*, there are 253 – 77 = 176(= $E_{2,1}$) octads containing *x* but not *y*. If the chosen element is *y*, then there are also 176 octads containing *y* but not *x*. Thus among those 506 octads which do not contain a particular element, there are 506 – 176 = 330(= $E_{2,0}$) octads which do not contain that particular element and another element of Ω. In general, we have $E_{i,j} = E_{i+1,j} + E_{i+1,j+1}$ which will give us $E_{i+1,j} = E_{i,j} - E_{i+1,j+1}$. In this way, we get Table 3.1.1 (Leech Table).

Remark : The first six rows of Table 3.1.1 has a more general interpretation. $E_{i,j}$ can mean the number of octads containing *j* elements out of any fixed *i* elements of Ω. But for the last three rows of Table 3.1.1 where *i* = 6, 7 or 8, $E_{i,j}$ only valid if the fixed *i* elements are chosen from an octad, since not every *i* element (where *i* = 6, 7 or 8) of Ω are contained in an octad.

In particular, from the bottom line of Table 3.1.1, $E_{8,0}, E_{8,2}, E_{8,4}$ and $E_{8,8}$ are nonzero integers. It shows that a fixed octad intersects other octads(including itself) in 0, 2, 4 or 8 elements. For example $E_{8,0}$ = 30 means for a chosen 8 element (from an octad, which itself is also an octad), there are 30 octads disjoint from this octad. This will be discussed in detail in Section 4.3 of Chapter 4.

3.2 Construction

Let Ω be a 24-element set. From Theorem 2.1.16, $P(\Omega)$ is a vector space over the field Z_2 under addition defined as symmetric difference and scalar multiplication defined as $\alpha \cdot x = \begin{cases} x, & \alpha = 1 \\ \phi, & \alpha = 0 \end{cases}$ where $\alpha \in Z_2, x \in P(\Omega)$.

We produce a subspace, **C**, of $P(\Omega)$. The subsets ($\neq \phi$) of smallest size in this subspace have size eight. Then we shall show that **C** contains just 759 of these subsets of size eight or octads. No two distinct octads can have five points or more in common. Also any five points of Ω must lie in an octad. Thus the set of octads must form a Steiner system S(5, 8, 24).

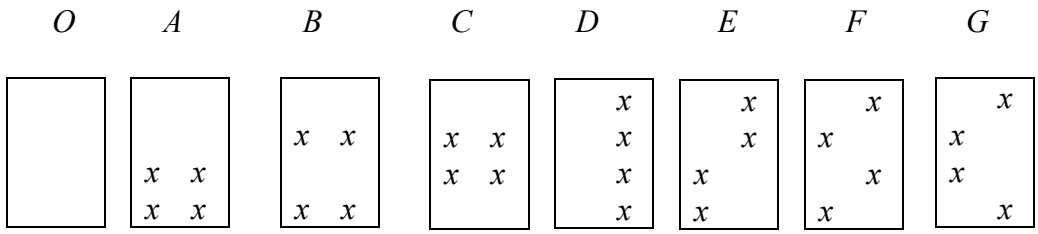
Theorem 3.2.1 There exists a Steiner System S(5, 8, 24).

Proof. Let Ω be a 24-element set. Let Λ be an 8-element subset of Ω. P(Λ) is a vector space over the field Z_2 under addition and scalar multiplication defined as above. We may think of Λ as a set containing 8 elements, say $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$ and represent it as $\begin{bmatrix} x_1 & x_5 \\ x_2 & x_6 \\ x_3 & x_7 \\ x_4 & x_8 \end{bmatrix}$ or $\begin{bmatrix} x & x \\ x & x \\ x & x \\ x & x \end{bmatrix}$.

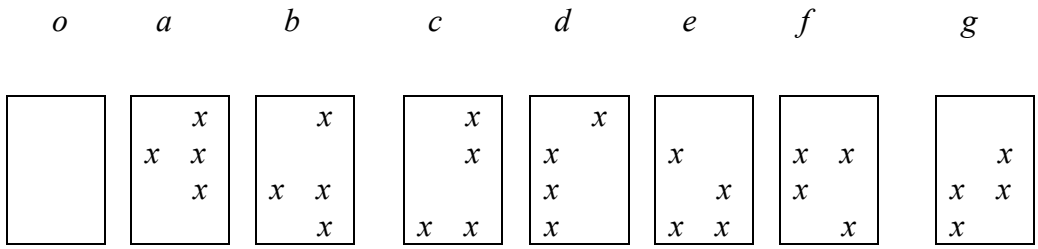
Consider the following two 3-dimensional subspaces P and L of $P(\Lambda)$, whose members are all tetrads (4-element subsets) and P $\cap$ L = O (or o). There are 8 (= 2^3) tetrads in

each 3-dimensional subspace of P (Λ). For each member of P and L, we may use drawing to represent them as follow

P =



L =



Note that P is spanned by *A, B* and *D* while L is spanned by *a, b* and *c*.

We want to show that any member of L ($\neq o$) defines a unique 2-dimensional subspace or *line* of P; namely the set of members of P that it cuts evenly at 0 or 2 points. For example, *a* of L defines a line of P which contains *O, B, E* and *G*. $\{B, E\}$ spans this 2-dimensional subspace of P. Note that $G = B + E$. After checking all members of L ($\neq o$), we have the following observations.

a of L cuts *O, B, E* and *G* evenly.

b of L cuts *O, C, E* and *F* evenly.

c of L cuts *O, A, F* and *G* evenly.

d of L cuts *O, A, B* and *C* evenly.

e of L cuts *O, C, D* and *G* evenly.

f of L cuts *O, A, D* and *E* evenly.

g of L cuts *O, B, D* and *F* evenly.

A member of L ($\neq O$) cuts exactly four members of P evenly. However no two members of L($\neq o$) cut the same four members of P evenly. On the other hand, we count the number of 2-dimensional subspaces or lines of P. Any set of two non-empty elements of P can be the basis for a line of P. But there are three different bases which span the same line. So the number of lines of P is 7 ($= \binom{7}{2} \Big/ \binom{3}{2}$) which is the same as the number of members of L ($\neq o$). Thus the members of L ($\neq O$) are in 1-1 correspondence with the lines of P. And we can say that any member of L ($\neq o$) defines a unique 2-dimensional subspace or line of P. We call P the point-space and L the line-space.

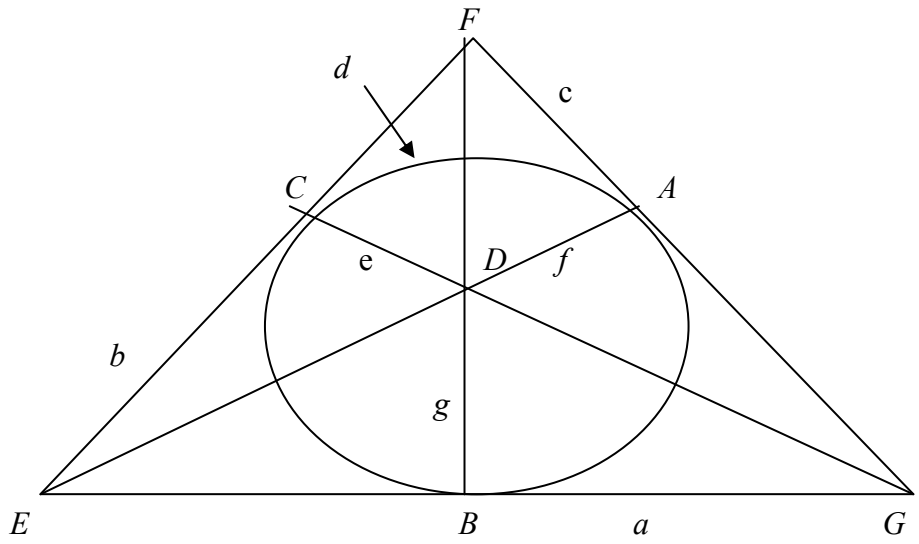


Figure 3.2.1

Let say $c \in L$ corresponds to the line l of P. By abuse of notation, we let $A \in c$ to denote A is a point of l. For $B \notin e$, it means B is not on the line of e. For $X \in$ P and $t \in$ L, if $X \in t$, then the cardinality of $(X + t)$ is 4 since every member of L cuts evenly (0 or 2) at the members of P which correspond to it. For those members of P which are not corresponding to $t \in$ L, t cuts them oddly at 1 or 3 points. Thus the cardinality of $(X + t)$, if $X \notin t$, is either 6 or 2 respectively. According to the observations before, we show this correspondence in Figure 3.2.1.

Here we are going to make a remark that we will need it later. For distinct nonzero X, Y, Z in P, $X + Y + Z = O$ (i.e. $Z = X + Y$) if and only if Z belongs to the line spanned by X and Y, if and only if X, Y, Z belong to the same line.

Let the complement of $X \in$ P be denoted X'. Observe that set Q which is spanned by O', A, B, D form a vector space of dimension four over Z_2 where addition and scalar multiplication are defined as above. Notice that for $X \in$ P and $t \in$ L, if $|X + t| = 4$, then t must also cut X' evenly and so we have $|X' + t| = 4$. Else if $|X + t| = 2$, t cuts those X oddly at 3 points. Thus t must cut X' at 1 point, and we have $|X' + t| = 6$. And if $|X + t| = 6$, then $|X' + t| = 2$.

Consider the vector space (Q + L). From Theorem 2.1.8, (Q + L) is the direct sum of Q and L since Q $\cap$ L = O (or o). And from Theorem 2.1.12, we know that dimension of (Q + L) is 7 (= 4 + 3 – 0). So there are 2^7 elements in (Q + L). From the above observations, all elements in (Q + L) are even subsets of Λ. On the other hand, from Theorem 2.1.15, there are $2^7 (= 2^8 / 2)$ even subsets of Λ. Therefore it is