Maram Alosaimi

9503596

M_{24}

Pure Mathematics and Mathematical Logic

May 2017

Prof. Peter Rowley

1 Introduction

The Mathieu groups are $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, which are one family of the 26 sporadic finite simple groups. They were discovered by the French mathematician Emile Mathieu (see figure 1). Furthermore, the first expression of simplicity and uniqueness of Mathieu groups was in 1930's in a paper by Witt, and a Steiner system was describled in this paper. Now, we are normally using the system to describe these groups. The largest Mathieu group is M_{24} which is 5-transitive of 24-point, and it could be defined as a group of preserved permutations of Steiner system $S(5, 8, 24)$. Notice that some of $M'_{24}s$ simple subgroups are $M_{23}, M_{22}, M_{12}, M_{11}$. This paper will start by introducing some basic facts, moving to the definition of Steiner system and some of its properties, followed by discussing the Steiner system $S(5, 8, 24)$, and then presenting the Miracle Octad Generator (MOG). Then we will end by introducing the concept of M_{24}. Finally, the main two sources for this paper are (An introduction to Steiner systems by M. Grannell and T. Griggs) and (A new combinatorial approach to M_{24} by R. Curtis).

Group	Order	Discovered by	Date
M_{11}	$2^4.3^2.5.11$	Mathieu	1873
M_{12}	$2^6.3^3.5.11$	Mathieu	1873
M_{22}	$2^7.3^2.5.7.11$	Mathieu	1873
M_{23}	$2^7.3^2.5.7.11.23$	Mathieu	1873
M_{24}	$2^{10}.3^3.5.7.11.23$	Mathieu	1873

Figure 1: The Mathieu groups

2 Preliminaries

2.1 Definition

$GF(2)$ is a finite field with 2 elements $\{0, 1\}$.

2.2 Definition

A set that contains four elements is called a tetrad.

2.3 Definition

Let V is a non-empty set and K is a field. Then V is called a vector space over K if V is an abelian group under addition and it is closed under a scalar multiplication, let $\lambda, \beta \in F, v, v_1, v_2 \in V$, then

I) $(\lambda + \beta)v = \lambda v + \beta v$.

II) $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$.

III) $(\lambda\beta)v = \lambda(\beta v)$.

IV) $1v = v$.

2.4 Definition

Let G be a group and $N \leq G$, then N is a normal subgroup, if for all $g \in G$ we have $N^g = N$.

2.5 Definition

A non-trivial group G is called simple if it has no proper non-trivial normal subgroups.

2.6 Definition

An action of a group G on a non-empty set Ω is a binary operation $* : \Omega \times G \to \Omega$, such that for all $\alpha \in \Omega$, $\alpha * 1 = \alpha$ and $(\alpha * g) * h = \alpha * (gh)$ for all $g, h \in G$. The degree of action G on Ω is the cardinality of Ω.

2.7 Definition

Let G act on a set Ω and $\alpha \in \Omega$. Then $\alpha^G = \{\alpha g | g \in G\} \subseteq \Omega$ is called the orbit of α under G.

Let G be a group acting on a non-empty set Ω.

- ### 2.8 Definition

  Let $\alpha \in \Omega$ and then $G_\alpha = \{g \in G | \alpha g = \alpha\}$ is called the stabiliser of α.

- ### 2.9 Definition

  G acts transitively on Ω if G has only one orbit. (That is $\alpha^G = \Omega$ for $\alpha \in \Omega$.)

- ### 2.10 Definition

  A group G acts k-transitively precisely if for any two sequences of k distinct points from Ω, say $(\alpha_1, \alpha_2, ..., \alpha_k)$ and $(\beta_1, \beta_2, ..., \beta_k)$ there is a group element $g \in G$ such that $\alpha_i g = \beta_i$ for each i, where $1 \leq i \leq k$.

- ### 2.11 Definition

  Let G be k-transitive, and for every k non repeating elements $\alpha_1, \alpha_2, ..., \alpha_k \in \Omega$, $g_1, g_2 \in G$ satisfy $\alpha_i g_1 = \alpha_i g_2$ for all $i = 1, ..., k$, and $g_1 = g_2$, then we say G acts sharply k-transitive on Ω.

2.12 Definition

Let X, Y be sets, then symmetric difference defines as $X + Y = Z$, where $Z = \{x : (x \in X \wedge x \notin Y) \vee (x \notin X \wedge x \in Y)\}$ or $Z = (X \setminus Y) \cup (Y \setminus X)$.

2.13 Definition

Let G and K are groups $\varphi : G \to K$ is a group homomorphism if for all $g_1, g_2 \in G$, $(g_1 g_2)\varphi = (g_1)\varphi(g_2)\varphi$.

3 Steiner system

3.1 Definition

A Steiner system $S(t, k, v)$ is a set of k-element subsets of a base set which is a set of v elements and any t-element subset of the base set appears in precisely one of the k-element subsets which are called blocks.

3.2 Theorem

If there exists an $S(t, k, v)$, then there exists an $S(t-1, k-1, v-1)$.

Proof
Suppose $S(t, k, v)$ exists, Ω is a base set and α is a fixed element in Ω. Then remove all the blocks which do not contain α, so the remaining blocks contain α and $t-1$ elements which appear precisely once in a block. By removing α from Ω and the blocks we obtain that $|\Omega \setminus \{\alpha\}| = v-1$, and the size of blocks is $k-1$. Hence this is an $S(t-1, k-1, v-1)$.

3.3 Theorem

If there exists an $S(t, k, v)$. Then $\binom{k}{t}$ divides $\binom{v}{t}$, and the number of blocks is $\binom{v}{t} / \binom{k}{t}$.

Proof
Suppose $S(t, k, v)$ exists, $|\Omega| = v$ and $X \subseteq \Omega$ with $|X| = k$, then the number of all subsets of size t of X is $\binom{k}{t}$. By assuming there are n sets of size k, and since any t-element lies in only one k-element, this implies that $n \times \binom{k}{t} = \binom{v}{t}$ and n is an integer, hence $\binom{v}{t} / \binom{k}{t}$.

3.4 Corollary

If there exists an $S(t, k, v)$, then $\binom{k-i}{t-i}$ divides $\binom{v-i}{t-i}$ for each $i = 0, 1, 2, ..., t-1$.

Proof:
Indeed by using Theorem (3.2) there exists $S(t-i, k-i, v-i)$ for each $i = 0, 1, 2, ..., t-1$. Then apply Theorem (3.3).

3.5 Example

In a Steiner system $S(2,3,9)$, the base set is Ω which has nine elements and for convenience suppose $\Omega = \{1,2,3,4,5,6,7,8,9\}$ with positive integers. Then our blocks have size 3 with the property that any pair lies in only one block. Notice that the number of blocks from Theorem (3.3) is $\binom{9}{2}/\binom{3}{2} = 12$, and the blocks are $\{1,2,3\}$, $\{4,5,6\}$, $\{7,8,9\}$, $\{1,4,7\}$, $\{2,5,8\}$, $\{3,6,9\}$, $\{1,5,9\}$, $\{2,6,7\}$, $\{3,4,8\}$, $\{2,4,9\}$ $\{3,5,7\}$ and $\{1,6,8\}$.

3.6 Example

In a Steiner system $S(3,4,8)$, the base set is Ω which has eight elements and for convenience suppose $\Omega = \{A,B,C,D,E,F,G,H\}$. Then our blocks have size 4 with property that any 3-element lies in only one block. Notice that the number of blocks from Theorem (3.3) is $\binom{8}{3}/\binom{4}{3} = 14$, and the blocks are $\{A,B,C,H\}, \{A,D,E,H\}, \{A,F,G,H\}, \{B,D,F,H\}, \{B,E,G,H\}, \{C,D,G,H\}$, $\{C,E,F,H\}, \{D,E,F,G\}, \{B,C,F,G\}, \{B,C,D,E\}, \{A,C,E,G\}, \{A,C,D,F\}$ $\{A,B,D,G\}$ and $\{A,B,E,F\}$.

3.7 Corollary

The $S(2,3,7)$ exists. This is clear from Theorem (3.2) and existence of $S(3,4,8)$.

3.8 Remark

It is not necessary there is a Steiner system for any three integers numbers as an example $S(2,3,8)$ is not a Steiner system since $\binom{3}{2}$ does not divide $\binom{8}{2}$ which contradiction with Theorem (3.3).

4 Steiner system S(5,8,24)

4.1 Definition

A Steiner system $S(5,8,24)$ is a set of all sets of size 8, which are subsets of a set of size 24 elements, say Ω with property that any subset of size 5 of Ω appears in only one of the 8-element sets which are called octads. (This means that $S(5,8,24) = \{B \subseteq \Omega : \forall X \subseteq \Omega \ \exists! B$ such that $X \subseteq B$ and $|B| = 8$, where $|X| = 5$ $\}$.)

4.2 Theorem

A Steiner system $S(5,8,24)$ exists.

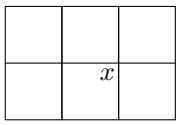
- The first claim is that the power-set of 24-element set is a vector space with 24 dimensions over $GF(2)$, and the addition operation is defined by symmetric difference in $\mathcal{P}(\Omega)$.

Proof
Suppose $\Omega = \{a_1, a_2, a_3, a_4, ..., a_{24}\}$, and V is a vector space with 24 dimensions over $GF(2)$, which has a standard basis $\{(1,0,0,....,0,0),....,(0,0,0,....,0,1)\}$. Moreover, the operation is symmetric difference. Now define a map,

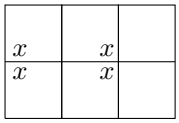
$$\varphi : \mathcal{P}(\Omega) \to V \quad \text{,by}$$

$$Y \to (i_1, .., i_j, .., i_{24}), \qquad \begin{array}{ll} i_j = 1 & if\, a_j \in Y \\ i_j = 0 & \text{if } a_j \notin Y \end{array}$$

We need to show that φ is surjective, injective and a group homomorphism, let Y, X be subsets of Ω and $(Y)\varphi = (i_1, .., i_j, .., i_{24}) = (X)\varphi = (k_1, .., k_j, .., k_{24})$. This implies that $i_j = k_j$ for all $1 \leq j \leq 24$, and $i_j = 1 = k_j$ for some j hence $a_j \in X$ and $a_j \in Y$, thus, $X = Y$. Therefore, φ is an injective function. Since $|V| = |\mathcal{P}(\Omega)| = 2^{24}$ and φ is an injection, this implies that φ is a surjective function. Now, we need to show that φ is a group homomorohism, suppose $X, Y \in \mathcal{P}(\Omega)$, and $X + Y = Z = \{a_j : a_j \in X \setminus Y \text{ or } a_j \in Y \setminus X\}$, hence $(X + Y)\varphi = (Z)\varphi = (t_1, t_2, ..., t_j, ...t_{24})$, where $t_j = 1$ if $k_j \neq i_j$ and zero otherwise. This is the sum of $(k_1, k_2, ..., k_j, ...k_{24}) + (i_1, i_2, ..., i_j, ...i_{24}) = (X)\varphi + (Y)\varphi$. Moreover, it is easy to see that $(\lambda X)\varphi = \lambda(X)\varphi$ where $\lambda \in GF(2) = \{0, 1\}$ and $X \in \mathcal{P}(\Omega)$. Thus, $\mathcal{P}(\Omega) \cong V$. As a result, $\mathcal{P}(\Omega)$ is a vector space over $GF(2)$ with basis $\{e_1, ..., e_{24}\}$, where,

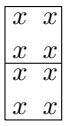
$e_i =$  $\to (0, 0, .., 1, ..0)$, where $i = 1, 2, 3, .., 24$

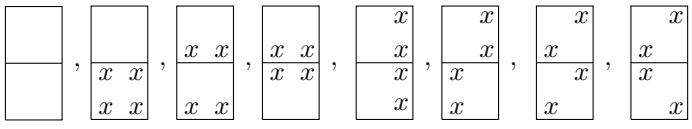
4.3 Example

$X = \{a_2, a_3, a_{14}, a_{15}\} =$  $\to (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, .., 0)$

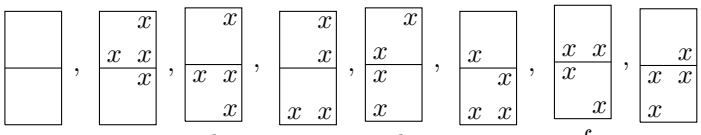
- The second claim is that we need to produce a subspace $\mathscr{C}$ of $\mathcal{P}(\Omega)$ such that $\mathscr{C} = \{X \in \mathcal{P}(\Omega) : |X| \geq 8\}$. Moreover, $\mathscr{C}$ contains 759 octads, and the set that contains all these is called $\mathscr{C}_8$ which is $S(5, 8, 24)$. Notice that if an $S(5, 8, 24)$ exists, then from Theorem (3.3) there are $\binom{24}{5} \diagup \binom{8}{5} = 759$ octads.

Proof

Let $\Lambda =$  be a set of 8 elements and consider $\mathcal{P}(\Lambda)$ as a 8-dimensional vector space over $GF(2)$ as before. Now, suppose we have any two subspaces of $\mathcal{P}(\Lambda)$, say P, L which are 3-dimensional, whose members are tetrads, and $P \bigcap L = \emptyset$. We may assume P and L as following.

$P =$ 

$0 \quad A \quad B \quad C \quad D \quad E \quad F \quad G$

$L =$ 

$o \quad a \quad b \quad c \quad d \quad e \quad f \quad g$

It can be seen from table 1, that $(P, *)$ is an abelian group, and it is closed under multiplication by λ, where $\lambda \in GF(2) = \{0, 1\}$. Hence P is a subspace of $\mathcal{P}(\Lambda)$ over $GF(2)$.

$*$	0	A	B	C	D	E	F	G
0	0	A	B	C	D	E	F	G
A	A	0	C	B	E	D	G	F
B	B	C	0	A	F	G	D	E
C	C	B	A	0	G	F	E	D
D	D	E	F	G	0	A	B	C
E	E	D	G	F	A	0	C	B
F	F	G	D	E	B	C	0	A
G	G	F	E	D	C	B	A	0

Table 1

Similarly, it can be seen from table 2, that $(L, *)$ is an abelian group, and it is closed under multiplication by λ, where $\lambda \in GF(2) = \{0, 1\}$. Hence L is also a subspace of $\mathcal{P}(\Lambda)$ over $GF(2)$.

$*$	0	a	b	c	d	e	f	g
0	0	a	b	c	d	e	f	g
a	a	0	f	e	g	c	b	d
b	b	f	0	g	e	d	a	c
c	c	e	g	0	f	a	d	b
d	d	g	e	f	0	b	c	a
e	e	c	d	a	b	0	g	f
f	f	b	a	d	c	g	0	e
g	g	d	c	b	a	f	e	0

Table 2

4.4 Remark

I) P is called the point-space, and L is called the line-space.

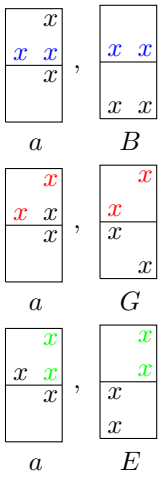
II) Intersection of any two members of P or (L) is a subset of size 2. (This means that if $X, Y \in P$ or (L), then $|X \bigcap Y| = 2$.)

III) Any three linearly independent of elements of P or (L) can be its basis. For example, $A, B, D \in P$ are linearly indepentent, thus $\{A, B, D\}$ can be a basis of P.

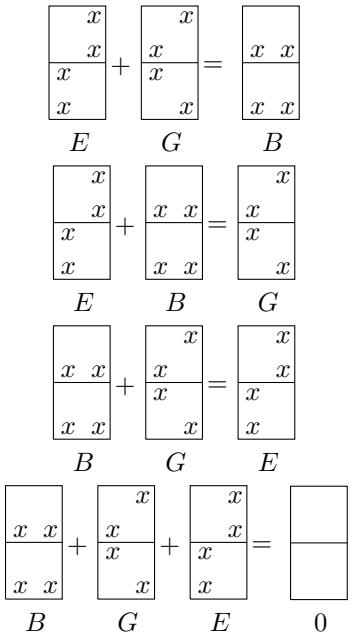
IV) For any member of L, say t, there is a one-to-one correspandence to a 2-dimensional vector space, whose members are from P. (This means that for any member of L there are three members of P, which have only two common points with the member of L and it has dimension two, because it is generated by any two non-zero elements, whereas the third element is their addition (see figure 2)).

4.5 Example

To show that $\{0, B, G, E\}$ is a 2-dimenisonal vector space of P over $GF(2)$. That is correspondence to a, firstly, we need to check common points between them.



So there are two common points between a and each non-zero member of the 2-dimensional vector space. Movreover, $\{0, E, B, G\}$ is a vector subspace of $\mathscr{C}$, since it is an abelian group, and it is closed under multiplication by a scalar. Notice that each non-zero element has order two, hence an inverse is the element itself. And it is two dimensional, since it is generated by any two non-zero members, say $\{E, B\}$, whereas, $G = E + B$.



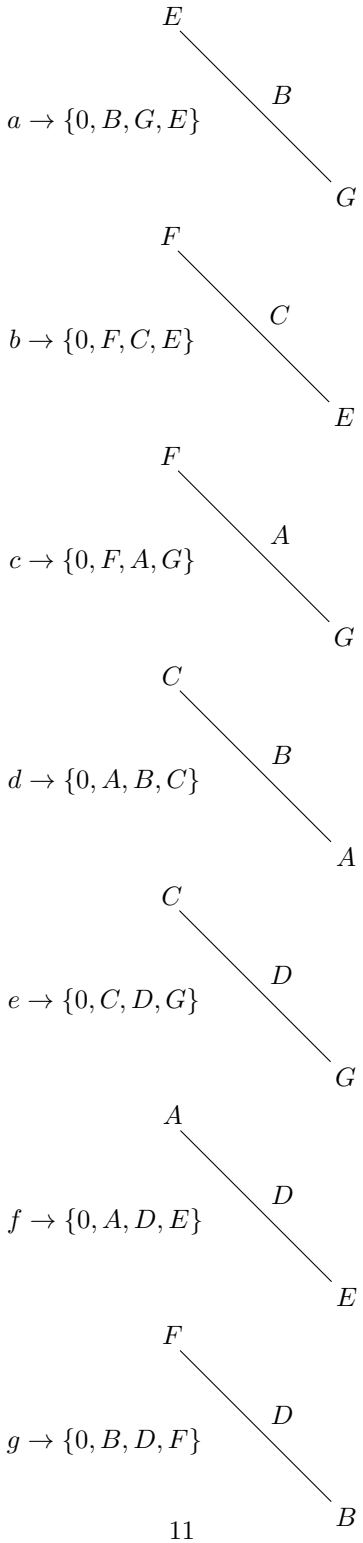

E
B
a → {0, B, G, E}
G
F
C
b → {0, F, C, E}
E
F
A
c → {0, F, A, G}
G
C
B
d → {0, A, B, C}
A
C
D
e → {0, C, D, G}
G
A
D
f → {0, A, D, E}
E
F
D
g → {0, B, D, F}
B

Figure 2

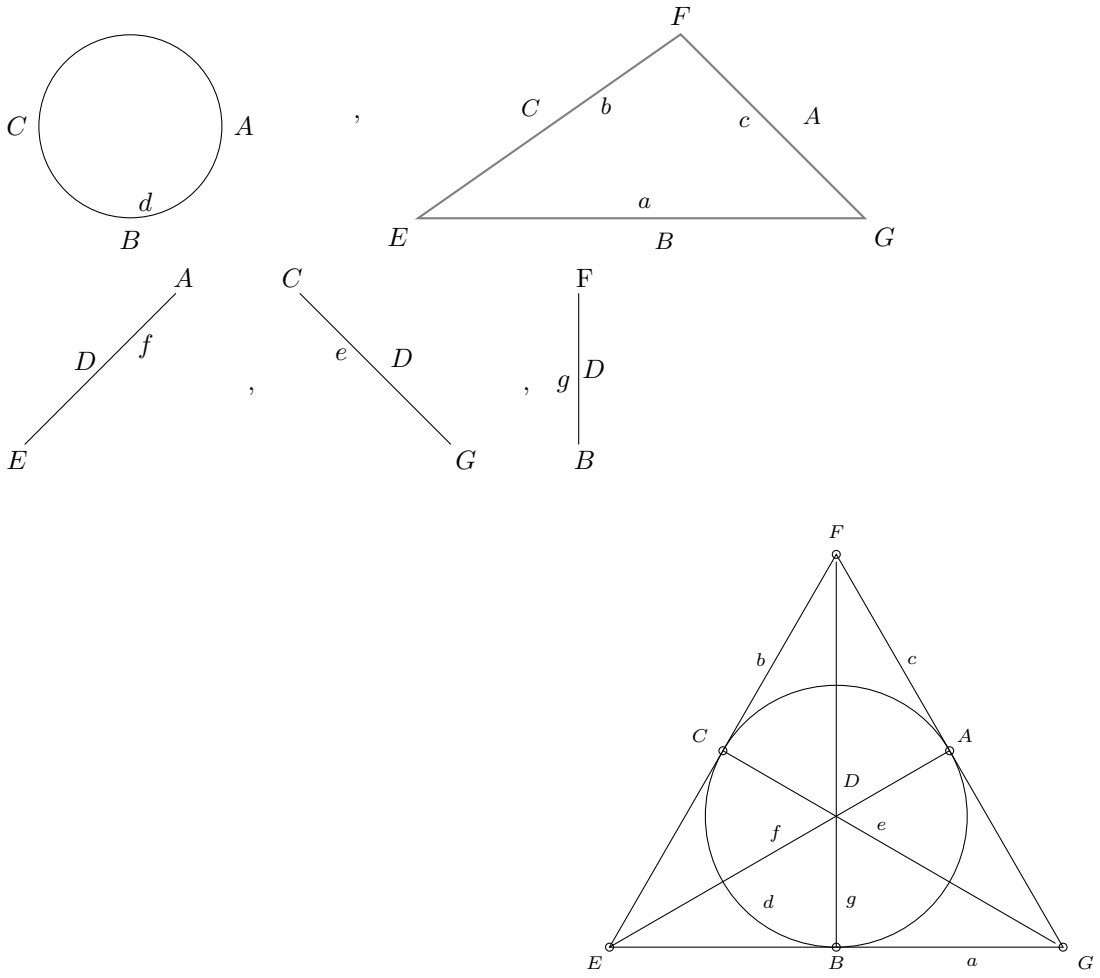
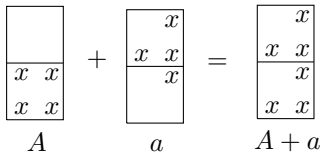


Figure 3: The one-to-one correspondence

4.6 Remark

I) Saying $X \in t$, if $|X + t| = 4$, and $X \notin t$ if $|X + t| = 2$ or 6. In other words, $X \in t$ if $|X \bigcap t| = 2$, $X \notin t$ if $|X \bigcap t| = 1$ or 3.

4.7 Example

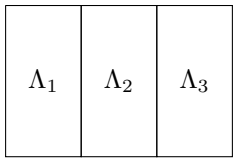


$A \quad a \quad A + a$

. This implies to $A \notin a$

II) From (I) notice that any even subset of Λ can be expressed uniquely as $(X + t)$ or $(X' + t)$, where X' is a subset of Λ, and $X + X' = \Lambda$, X' is called the complement of X.

Now, consider three copies of Λ, and define the 12- dimensional space $\mathscr{C}$ of $\mathcal{P}(\Omega)$.



Such that $\{[(XorX')(YorY')(ZorZ')]_t : X, Y, Z \in P,\, t \in L, X + Y + Z = 0\}$, it is called $\mathscr{C} - set$, where

$$[(XorX')(YorY')(ZorZ')]_t = \begin{array}{|c|c|c|} \hline XorX' & YorY' & ZorZ' \\ + & + & + \\ t & t & t \\ \hline \Lambda_1 & \Lambda_2 & \Lambda_3 \end{array}$$

4.8 Example

Let $A, B, C \in P$, hence $A + B + C = 0$, and $e \in L$, then

$$[ABC]_e = [A + e, B + e, C + e] = \begin{array}{|c|c|c|} \hline x & x & x \\ \hline x & x & x \\ \hline & & x \quad x \\ \hline \end{array}$$

Investigation the size of members of $\mathscr{C}$ − *set*

		Intersection with Λ_i		
		Λ_1	Λ_2	Λ_3
$[000]_0$	$\|0\| = 0$	0	0	0
$[0'00]_0$	$\|0\| = 0, 0' = \Lambda, \|0'\| = 8$	8	0	0
$[00'0]_0$	$\|0\| = 0, 0' = \Lambda, \|0'\| = 8$	0	8	0
$[000']_0$	$\|0\| = 0, 0' = \Lambda, \|0'\| = 8$	0	0	8
$[0'0'0]_0$	$\|0\| = 0, 0' = \Lambda, \|0'\| = 8$	8	8	0
$[0'00']_0$	$\|0\| = 0, 0' = \Lambda, \|0'\| = 8$	8	0	8
$[00'0']_0$	$\|0\| = 0, 0' = \Lambda, \|0'\| = 8$	0	8	8
$[0'0'0']_t$	$0' = \Lambda, \|0'\| = 8$	8	8	8
$[XX0]_0$	$\|X\| = 4$	4	4	0
$[X0X]_0$	$\|X\| = 4$	4	0	4
$[0XX]_0$	$\|X\| = 4$	0	4	4
$[X'X'0]_0$	$X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	0
$[X'0X']_0$	$X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	0	4
$[0X'X']_0$	$X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	0	4	4
$[XX0']_0$	$\|X\| = 4, 0' = \Lambda, \|0'\| = 8$	4	4	8
$[X0'X]_0$	$\|X\| = 4, 0' = \Lambda, \|0'\| = 8$	4	8	4
$[0'XX]_0$	$\|X\| = 4, 0' = \Lambda, \|0'\| = 8$	8	4	4
$[X'X'0']_0$	$X + X' = \Lambda, \|X\| = 4, \|X'\| = 4, 0' = \Lambda, \|0'\| = 8$	4	4	8
$[X'0'X']_0$	$X + X' = \Lambda, \|X\| = 4, \|X'\| = 4, 0' = \Lambda, \|0'\| = 8$	4	8	4
$[0'X'X']_0$	$X + X' = \Lambda, \|X\| = 4, \|X'\| = 4, 0' = \Lambda, \|0'\| = 8$	8	4	4
$[XX0]_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X0X]_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0XX]_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'X'0]_t$	$X + X' = \Lambda, X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'0X']_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0X'X']_t$	$X + X' = \Lambda, X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[XX'0]_t$	$X + X' = \Lambda, X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'X0]_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0XX']_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0X'X]_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X0X']_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'0X]_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[XX0']_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X0'X]_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0'XX]_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'X'0']_t$	$X + X' = \Lambda, X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'0'X']_t$	$X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0'X'X']_t$	$X + X' = \Lambda, X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[XX'0']_t$	$X + X' = \Lambda, X \in t, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X'X0']_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0'XX']_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[0'X'X]_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4
$[X0'X']_t$	$X \in t, X + X' = \Lambda, \|X\| = 4, \|X'\| = 4$	4	4	4

		Intersection with Λ_i		
		Λ_1	Λ_2	Λ_3
$[X'0'X]_t$	$X \in t, X + X' = \Lambda, \lvert X\rvert = 4, \lvert X'\rvert = 4$	4	4	4
$[XX0]_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	2	4
$[X0X]_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	4	2
$[0XX]_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	2	2
$[X'X'0]_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	6	4
$[X'0X']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	4	6
$[0X'X']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	6	6
$[XX'0]_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	6	4
$[X'X0]_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	2	4
$[0XX']_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	2	6
$[0X'X]_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	6	2
$[X0X']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	4	6
$[X'0X]_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	4	2
$[XX0']_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	2	4
$[X0'X]_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	4	2
$[0'XX]_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	2	2
$[X'X'0']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	6	4
$[X'0'X']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	4	6
$[0'X'X']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	6	6
$[XX'0']_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	6	4
$[X'X0']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	2	4
$[0'XX']_t$	$X \notin t, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	2	6
$[0'X'X]_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	4	6	2
$[X0'X']_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	2	4	6
$[X'0'X]_t$	$X \notin t, X + X' = \Lambda, \lvert X\rvert = 2, \lvert X'\rvert = 6$	6	4	2
$[XYZ]_0$	$X + Y + Z = 0, \lvert X\rvert = \lvert Y\rvert = \lvert Z\rvert = 4$	4	4	4
$[X'Y'Z']_0$	$X + Y + Z = 0, X \in t, \lvert X'\rvert = \lvert Y'\rvert = \lvert Z'\rvert = 4$	4	4	4
$[XYZ]_t$	$X + Y + Z = 0, X \in t, Y \in t, Z \in t, \lvert X\rvert = \lvert Y\rvert = \lvert Z\rvert = 4$	4	4	4
$[X'Y'Z']_t$	$X + Y + Z = 0, X \in t, Y \in t, Z \in t, \lvert X'\rvert = \lvert Y'\rvert = \lvert Z'\rvert = 4$	4	4	4
$[XYZ]_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X\rvert = 4, \lvert Y'\rvert = \lvert Z'\rvert = 6$	4	2	2
$[XY'Z]_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X\rvert = 4, \lvert Y'\rvert = 2, \lvert Z\rvert = 6$	4	6	2
$[XYZ']_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X\rvert = 4, \lvert Y\rvert = 2, \lvert Z'\rvert = 6$	4	2	6
$[XY'Z']_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X\rvert = 4, \lvert Y'\rvert = \lvert Z'\rvert = 6$	4	6	6
$[X'YZ]_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X'\rvert = 4, \lvert Y\rvert = \lvert Z\rvert = 2$	4	2	2
$[X'Y'Z]_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X'\rvert = 4, \lvert Y'\rvert = 6, \lvert Z\rvert = 2$	4	6	2
$[X'YZ']_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X'\rvert = 4, \lvert Y\rvert = 2, \lvert Z'\rvert = 6$	4	2	6
$[X'Y'Z']_t$	$X + Y + Z = 0, X \in t, Y \notin t, Z \notin t, \lvert X'\rvert = 4, \lvert Y'\rvert = \lvert Z'\rvert = 6$	4	6	6

Table 3

Thus, $\mathscr{C}_8$ can be obtained from $\mathscr{C} - set$ by taking shapes which intersect with $(\Lambda_1 + \Lambda_2 + \Lambda_3)$ in 8 points.

Case	Shapes	The number of Octads
1	$[0'00]_0, [00'0]_0, [000']_0$	$1 \times 3 = 3$
2	$[XX0]_0, [X0X]_0, [0XX]_0,\ [X'X'0]_0, [X'0X']_0, [0X'X']_0,$	$7 \times 12 = 84$
2	$[XX'0]_0, [X0X']_0, [0XX']_0,\ [X'X0]_0, [X'0X]_0, [0X'X]_0$	$7 \times 12 = 84$
3	$[XX'0]_t, [X0X']_t, [0XX']_t,\ [X'X0]_t, [X'0X]_t, [0X'X]_t$	$7 \times 4 \times 6 = 168$
4	$[XYZ]_t, [XZY]_t, [X'YZ]_t, [X'ZY]_t$	$7 \times 3 \times 3 \times 2 \times 4 = 504$

Table 4

Table 4 shows all possibilities for the octad's shape. In particular, the first case shows all possibilities for ordering $0, 0'$ and $t = 0$, which are three possibilities. The second case presents all the possibilities of ordering $X, X', 0$ and $t = 0$, which are 12 shapes times the number of ways of choosing $X \in P \setminus \{0\} = \{A, B, C, D, E, F, G\}$ which is 7. The third case shows all the possibilities of ordering $X, X', 0$ and $X \notin t \neq 0$, which are 6 shapes. And from figure 3, we can find out there are four possibilities to choose $t \in L \setminus \{0\} = \{a, b, c, d, e, f, g\}$, where $X \notin t$, $(|X + t| \neq 4)$, so it is $4 \times 6 \times 7$. The fourth case shows all the possibilities of ordering X, X', Y, Z and $X \in t \neq 0, Y \notin t, Z \notin t$ and $X + Y + Z = 0$, which are four shapes. Moreover, From figure 3, there are three possibilities to choose $t \in L \setminus \{0\} = \{a, b, c, d, e, f, g\}$, where $X \in t$, $X \in P \setminus \{0\}$. And there are three choices to choose $Y \in P \setminus \{0, X\} = \{A, B, C, D, E, F, G\}$ and there are two choices to choose $Z \in P \setminus \{0, X, Y\} = \{A, B, C, D, E, F, G\}$, hence $7 \times 3 \times 3 \times 2 \times 4$. Therefore, $|\mathscr{C}_8| = 3 + 84 + 168 + 504 = 759$ octads. Furthermore, it is satisfied that any 5-element lies in only one Octad of $\mathscr{C}_8 \subseteq \mathscr{C}$. (If it is not, then there exists $X, Y \in \mathscr{C}_8$ such that $|X| = 8$, $|Y| = 8$ and $|X \bigcap Y| = 5$, but this is impossible since that $|X + Y| \leq 6$, and $X + Y \notin \mathscr{C}$ which is a contradiction the fact that $\mathscr{C}$ is a vector space.) Hence, $S(5, 8, 24) = \mathscr{C}_8$, and $|S(5, 8, 24)| = 759$.

4.9 Definition

If X is an octad which not equal Λ_1, Λ_2 or Λ_3, then $|X \cap \Lambda_i| = 4$ for some $i = 1, 2, 3$. We called Λ_i a heavy brick for X. In this case $|X \cap (\Lambda_j + \Lambda_k)| = 4$ for $\{i, j, k\} = \{1, 2, 3\}$ and we called $X \cap (\Lambda_j + \Lambda_k)$ a square tetrad.

4.10 Example

$$[A'A0]_0 = \begin{array}{|cc|cc|cc|} \multicolumn{2}{c}{\Lambda_1'} & \multicolumn{2}{c}{\Lambda_2'} & \multicolumn{2}{c}{\Lambda_3'} \\ \hline x & x & & & & \\ x & x & & & & \\ \hline & & x & x & & \\ & & x & x & & \\ \hline \end{array}$$

It can be seen here $A' + 0$ is in Λ_1', and $A + 0$ is in Λ_2', whereas Λ_3' is empty. Since $|\Lambda_1'| = |\Lambda_2'| = 4$ a heavy brick and a square tetrad is either Λ_1' or Λ_2'.

4.11 Example

$$[0'A'A']_a = \begin{array}{|cc|cc|cc|} \multicolumn{2}{c}{\Lambda_1'} & \multicolumn{2}{c}{\Lambda_2'} & \multicolumn{2}{c}{\Lambda_3'} \\ \hline x & & x & & x & \\ & & & & & \\ \hline x & & & x & & x \\ x & x & & & & \\ \hline \end{array}$$

It can be seen that in Λ_1' is $0'+a = \Lambda+a = a'$ and $|\Lambda_1'| = 4$, wheras $|\Lambda_2+\Lambda_3'| = 4$. This implies that Λ_1' is the heavy brick and $(\Lambda_2' + \Lambda_3')$ is the square tetrad.

4.12 Example

$$[DE'A]_b = \begin{array}{|cc|cc|cc|} \multicolumn{2}{c}{\Lambda_1'} & \multicolumn{2}{c}{\Lambda_2'} & \multicolumn{2}{c}{\Lambda_3'} \\ \hline & & x & x & & x \\ & x & x & & & \\ \hline x & & x & & & \\ & & & & x & \\ \hline \end{array}$$

It can be seen that in Λ_2' is $E' + b$ and $|\Lambda_2'| = 4$, wheras $|\Lambda_1' + \Lambda_3'| = 4$. This implies that Λ_2' is the heavy brick and $(\Lambda_1' + \Lambda_3')$ is the square tetrad.

4.13 Remark

I) There are 70 possibilities to arrange four points in eight places (so there are 70 heavy bricks). To see this let x_1, x_2, x_3, x_4 our four points in a heavy brick. Then, there are

1	2
3	4
5	6
7	8

$x_1 \to 8$ Choices to put x_1 in any of the eight squares.
$x_2 \to 7$ Choices to put x_2 in any of the eight squares
$x_3 \to 6$ Choices to put x_3 in any of the eight squares
$x_4 \to 5$ Choices to put x_4 in any of the eight squares

Figure 4

But, $x_1 = x_2 = x_3 = x_4$, hence the ordering is not important and there are repeated brick so to avoid this in figure 4 we need to divide by 4!. Therefore, $(8 \times 7 \times 6 \times 5)/4! = 70$ heavy bricks.

II) All possibilities to arrange four points in 16 places (square tetrad) is 140 bricks, assuming the property that the number of points in each columns should be equal (mod 2). (This means that $2k \equiv 0$, where $k \in \mathbb{Z}$), and rows similarly.

Shapes of columns

	1	2	3	4
a	1	2	9	10
b	3	4	11	12
c	5	6	13	14
d	7	8	15	16

$(4\ 0\ 0\ 0)\times 4$, with $(1\ 1\ 1\ 1)\times 1$ one point in each row
$(2\ 2\ 0\ 0)\times 6$, with $(2\ 2\ 0\ 0)\times 6$ shapes of rows
$(2\ 2\ 0\ 0)\times 6$, with $(1\ 1\ 1\ 1)\times 6$ one point in each row
$(1\ 1\ 1\ 1)\times 24$, with $(1\ 1\ 1\ 1)\times 1$ one point in each row
$(1\ 1\ 1\ 1)\times 6$, with $(2\ 2\ 0\ 0)\times 6$ shapes of rows
$(1\ 1\ 1\ 1)\times 1$, with $(4\ 0\ 0\ 0)\times 4$ shapes of rows

Hence $4 + (6 \times 6) + (6 \times 6) + 24 + (6 \times 6) + 4 = 140$ brick tetrad.

Figure 5

4.14 Example

Let the shape of columns is (4 0 0 0) and the shape of rows is (1 1 1 1), all possibilities to arrange these shaps in 16 places are

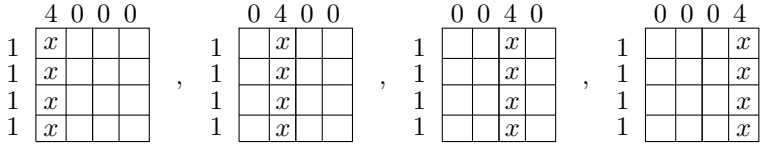


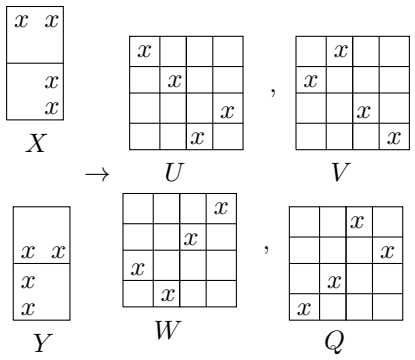
Figure 6

4.15 Definition

A picture contains a group of heavy bricks and a group of square bricks. Moreover, the 35 pictures are obtained from the one-to-one correspondence that is from 70 heavy bricks that are divided into two groups, (saying $|X| = |Y| = 4$ in the same group if $X + Y = \Lambda$, as in figure 7), to 140 square tetrads that are divided into four groups, (saying $|U| = |V| = |W| = |Q| = 4$ in the same group if $U + V + W + Q = \Lambda + \Lambda$, as in figure 7).

4.16 Example

This is picture (1) in figure 8 which consists of a correspondent group of heavy bricks to a group of square bricks.



Picture (1)

Where

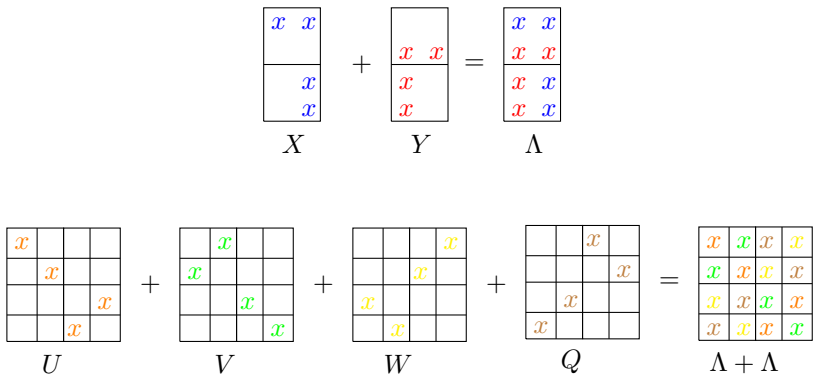


Figure 7

5 The Miracle Octad Generator (MOG)

5.1 Definition

The Miracle Octad Generator **(MOG)** is 36 pictures which are one of them shows named of points, whereas 35 pictures contain pair of brick tetrads and the corresponding group of square bricks. Moreover, taking any one of the pair together with any one of square bricks in the same group is an octad.

5.2 Remark

I) There are all the symmeries bodily permuting of $\Lambda_1, \Lambda_2, \Lambda_3$ in **MOG** diagram.

II) Black and white present two different heavy bricks, and in the same picture, black square, white square, black circle and white circle present four different square tetrads.

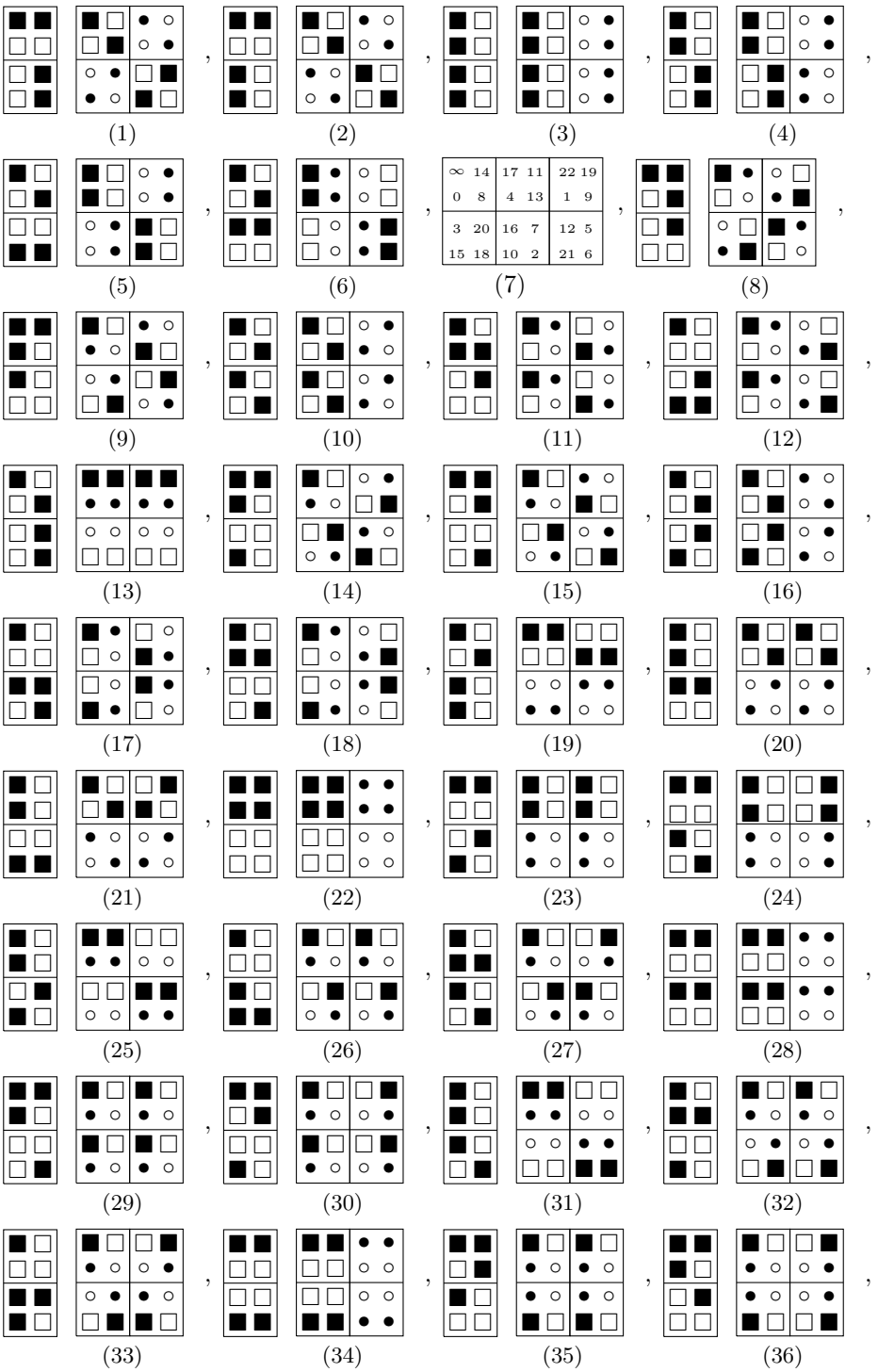
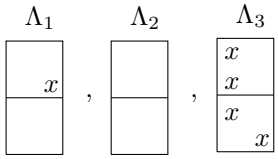


Figure 8: The Miracle Octad Generator **(MOG)**

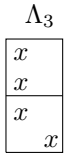
5.3 Example

To find the octad that contains $(22, 1, 12, 6, 8)$ in **MOG**, we need to do

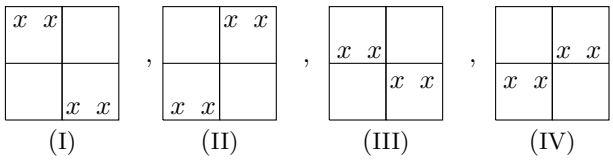
- Step 1: We should assign the points in $\Lambda_1, \Lambda_2, \Lambda_3$ by using picture (7) in **MOG**.



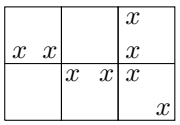
- Step 2: Finding the heavy brick which here is Λ_3 (since $|\Lambda_3| = 4$) and it is in picture (31).



- Step 3: Looking for square tetrad that contains (point 8), but in picture (31) there are four square tetrads



Hence 8 in Λ_1, this implies that (III) is the square tetrad which contains $(22, 1, 12, 6, 8)$, and then our octad is

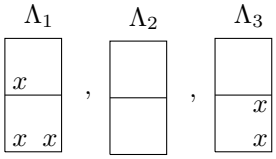


$=(0, 8, 16, 7, 22, 1, 12, 6)$

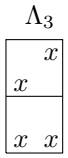
5.4 Example

To find the octad that contains $0, 15, 18, 5, 6$ in **MOG**, we need to do

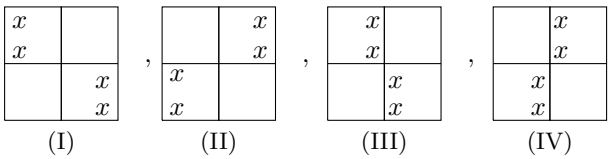
- Step 1: We should assign the points in $\Lambda_1, \Lambda_2, \Lambda_3$ by using picture (7) in **MOG**.



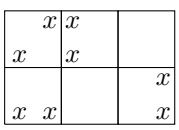
- Step 2: Finding the heavy brick which is Λ_1 (since $|\Lambda_1| = 3$), and is in one of these pictures (6), (8), (28) or (35), but Λ_3 should contain (points 5 and 6). Therefore, the heavy brick should be



- Step 3: Looking for square tetrad that contains (points 5 and 6), but in picture (6) there are four square tetrads



Since (points 5 and 6) are in Λ_3, this implies that (I) is the square tetrad which contains $(5, 6, 12, 4, 17)$ and then our octad is

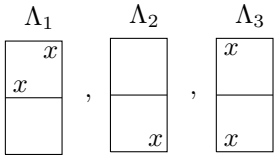


$=(0, 15, 14, 18, 17, 4, 5, 6)$

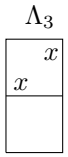
5.5 Example

To find the octad that contains $0, 14, 2, 22, 21$ in **MOG**, we need to do

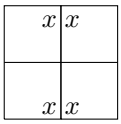
- Step 1: We should assign the points in $\Lambda_1, \Lambda_2, \Lambda_3$ by using picture (7) in **MOG**.



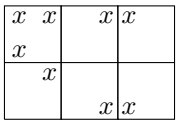
- Step 2:
  Finding the heavy brick which is either Λ_1 or Λ_3, since $|\Lambda_1| = 2 = |\Lambda_3|$. If Λ_3 is the heavy brick, then it is in one of these pictures (2, 3, 5, 12, 14, 16, 19, 21, 23, 25, 26, 30, 33 and 34). But all the corresponding square tetrads in these pictures do not contain (points 14, 0 and 2) in any of their square tetrads. Therefore, Λ_1 must be the heavy brick which is in pictures (5, 6, 9, 10, 12, 13, 14, 16, 17, 19, 22, 26, 29, 30 and 36). Since square tetrad must contain (points 2, 22 and 21). This implies that the picture must be (36). Hence, the heavy brick is



  And the square tetrad is



Hence our octad is



$=(\infty, 0, 14, 20, 11, 22, 2, 21)$

5.6 Corollary

Steiner systems $S(4,7,23)$ and $S(3,6,22)$ exist.

Proof
Indeed, we can obtain $S(4,7,23)$ from Theorem (3.2) and existence of $S(5,8,24)$. Moreover, the number of blocks from Theorem (3.3) is $\binom{23}{4}/\binom{7}{4} = 253$ blocks. Similarly, $S(3,6,22)$ can be obtained from Corollary (3.4) and existence of $S(5,8,24)$. The number of blocks from Theorem (3.3) is $\binom{22}{3}/\binom{6}{3} = 77$ blocks. In general, let $S_8 = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \}$ be an octad and $S_j = \{a_1, a_2, a_3, ..., a_j\}$, where $j \leq 7$. Figure 9 shows the number of octads intersecting S_i in S_j, where $(j+1)$ is the entry and $(i+1)$ is the line. As an example, let α, $\beta \in \Omega$ then there are $253 - 77 = 176$ octads that contain α not β.

759
506 253
330 176 77
220 120 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

Figure 9

5.7 Remark

I) The ninth line in figure 9 shows that any two octads intersect in 0, 2, 4 or 8 points.

II) There is another way to count how many octads contain i points which is $\binom{24-i}{5-i}/\binom{8-i}{5-i}$, where $0 \leq i \leq 4$. Moreover, it is 1 where $i \geq 5$.

5.8 Lemma

If $S, T \in \mathscr{C}_8$ and $|S \bigcap T| = 4$, then $S + T \in \mathscr{C}_8$.

Proof
Let $S = \{ a_1, a_2, ..., a_8\}, T = \{a_1, a_2, a_3, a_4, b_5, b_6, b_7, b_8\}$ be two octads, and suppose $T + S \notin \mathscr{C}_8$. Consider another octad, say W which contains (a_5, a_6, a_7, a_8, b_5). From Remark (5.7) there are no two octads which intersect in one point, so W contain a further point of T and not $a's$ since then $|S \bigcap W| \geq 5$, so say b_6. Similarly with W_1 that contains (a_5, a_6, a_7, a_8, b_7), say b_8. But now consider the octad, W_2 that contains (a_5, a_6, a_7, b_5, b_7). It must contain a further point of S, if $a_8 \in W_2$, then $|W_2 \bigcap W_1| \geq 5$, say a_1, but then W_2 must contain another point of T, if $a's$ is added, then $|S \bigcap W_2| \geq 5$, if b_8 is added, then $|W_2 \bigcap W_1| \geq 5$, if b_6 is added, then $|T \bigcap W_2| \geq 5$, in each case we reach to a contradiction, hence $T + S \in \mathscr{C}_8$.

5.9 Definition

Let $Y = Y_1 \cup Y_2 ... \cup Y_s$ be a decomposition of Y into disjoint sets Y_i, and $X \subseteq Y$, if $|Y_i \bigcap X| = r_i$ points, $1 \leq i \leq s$, then X cuts this decomposition as $r_1.r_2.....r_s$, and $|X| = r_1 + r_2 + ... + r_s$.

5.10 Corollary

There is a partition of the 24 points into 6 tetrads, which is an correspondence to each 4-point of Ω, say Y_i, $1 \leq i \leq 6$, then $\Omega = Y_1 \cup Y_2 \cup Y_3 \cup Y_4 \cup Y_5 \cup Y_6$, with $|Y_i| = 4, |Y_i + Y_j| = 8$, $i \neq j, 1 \leq i, j \leq 6$, and $Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$ is called a sextet.

5.11 Lemma

An octad cuts the 6 tetrads of a sextet $4^2.0^4$, 3.1^5 or $2^4.0^2$.

Proof
Let Y be a set of 24 points, $X \subseteq Y$, $|X| = 8$, and $Y = Y_1 \cup Y_2 \cup Y_3 \cup Y_4 \cup Y_5 \cup Y_6$. There are three cases,

Case 1 If $|Y_i \bigcap X| = 1$ point $1 \leq i \leq 6$, but $|X| = 8$, then there are two points left, if the two points in the same Y_i, say Y_1, then $|Y_1 \bigcap X| = 3$. Since $|(Y_i + Y_j) \bigcap X| = 2$ or $4, i \neq j, 1 \leq i, j \leq 6$. Hence X cuts Y_i as 3.1.1.1.1.1, wheras, if the two points in different Y_i, say Y_1, Y_2. Then $|(Y_1 + Y_3) \bigcap X| = 3$ contrdiction with Lemma (5.11).

Case 2 If $|Y_i \bigcap X| = 2$ points $1 \leq i \leq 6$, since $|X| = 8$, then there are only four Y_i, say Y_1, Y_2, Y_3, Y_4 which intersect with X in two points. Hence $|(Y_i + Y_j) \bigcap X| = 0, 2$ or $4, i \neq j, 1 \leq i, j \leq 6$. Hence X cuts Y_i as 2.2.2.2.0.0.

Case 3 If $|Y_i \bigcap X| = 4$ points $1 \leq i \leq 6$, since $|X| = 8$, then there are only two Y_i, say Y_1, Y_2 which intersect with X in four points. Hence $|(Y_i + Y_j) \bigcap X| = 0, 4$ or $8, i \neq j, 1 \leq i, j \leq 6$. Hence X cuts Y_i as 4.4.0.0.0.0.

5.12 Lemma

The intersection matrix for the tetrads of two sextets is one of the following:

$$\underset{\text{(I)}}{\begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}}, \underset{\text{(II)}}{\begin{pmatrix} 2 & 2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}},$$

$$\underset{\text{(III)}}{\begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}}, \underset{\text{(IV)}}{\begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}}$$

Proof

Let $Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$, and $Z_1, Z_2, Z_3, Z_4, Z_5, Z_6$ be the two sextets, by using Lemma (5.11) . Suppose that $Y_i + Y_j$ is an octads, where $i \neq j$, $1 \leq i, j \leq 6$ and Z_i with $1 \leq i \leq 6$ is a sextet, we get these matrices, where the entry in i^{th} row and j^{th} column is the intersection of Y_i and Z_j.

5.13 Example

$$\begin{array}{c} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \\ Y_6 \end{array} \begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ Z_1 & Z_2 & Z_3 & Z_4 & Z_5 & Z_6 \end{pmatrix}$$

Let $Y_1 + Y_2$ be an octad, then it cuts $Z_1 \cup Z_2 \cup Z_3 \cup Z_4 \cup Z_5 \cup Z_6$ as 4.4.0.0.0.0 and if our octad is $Y_1 + Y_6$, then it cuts $Z_1 \cup Z_2 \cup Z_3 \cup Z_4 \cup Z_5 \cup Z_6$ as 3.1.1.1.1.1.

5.14 Theorem

The Steiner system $S(5, 8, 24)$ is unique.

Proof
Suppose $\Omega = \{\infty, 0, 1, ..., 22\}$, and $O_1 \subseteq \Omega$ is an octad such that $x_1, x_2, x_3, x_4, x_5, x_6$ in O_1 and $x_7 \in \Omega \setminus O_1$. Now we can write $O_1 + \Omega$ in 4×6 array where the first two columns are O_1.

$x_1\, x_5$ $x_2\, x_6$	x_7	
x_3 x_4		

Now, we may assume S_∞ is a sextet that defines by the tetrad, $Y_x = \{x_1, x_2, x_3, x_4\}$, and by rearranging the un-named 17 points, we get this

$$S_\infty = \begin{array}{|cc|cc|cc|}\hline x & 0 & 1 & 2 & 3 & 4 \\ x & 0 & 1 & 2 & 3 & 4 \\ \hline x & 0 & 1 & 2 & 3 & 4 \\ x & 0 & 1 & 2 & 3 & 4 \\ \hline \end{array}$$

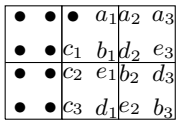
Notice that $S_\infty = Y_x \cup Y_0 \cup Y_1 \cup Y_2 \cup Y_3 \cup Y_4$, which means that S_∞ is a sextet. Moreover, O_1 cuts S_∞ as 4.4.0.0.0.0. Now consider the octad, say O_2 that contains x_2, x_3, x_4, x_5, x_7 which cuts S_∞ as 3.1.1.1.1.1, so we get this

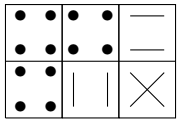
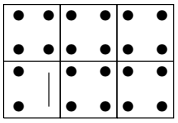
$$S_0 = \begin{array}{|cc|cc|cc|}\hline 0 & x & 1 & 1 & 1 & 1 \\ x & 0 & 2 & 2 & 2 & 2 \\ \hline x & 0 & 3 & 3 & 3 & 3 \\ x & 0 & 4 & 4 & 4 & 4 \\ \hline \end{array} \quad \text{is a sextet.}$$

Notice that from figure 9 the number of disjoint octads from O_1 is 30 octads. Now consider the octad, say O_3 that contains x_1, x_3, x_4, x_5, x_7, which cuts both S_∞ and S_0 as 3.1.1.1.1.1 such that $|O_3 \bigcap Y_x| = 3$ points, $|O_3 \bigcap Y_1| = |O_3 \bigcap Y_2| = |O_3 \bigcap Y_3| = |O_3 \bigcap Y_4| = 1$ point. This implies that

$$S_1 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 2 & 3 & 4 \\ 0 & 0 & 2 & 1 & 4 & 3 \\ \hline x & 0 & 3 & 4 & 1 & 2 \\ x & 0 & 4 & 3 & 2 & 1 \\ \hline \end{array} \quad \text{is a sextet.}$$

Notice that the group of permatuations that preserve the sextets S_∞, S_0 and S_1 is given by

$\pi =$ 

, $\sigma =$  , $\rho =$ 

Where dots denote fixed points and π is a 3-element taking $x_1 \to x_2 \to x_3 \to x_4 \to x_1$ where $x_i \in \{a_i, b_i, c_i, d_i, e_i\}$. Now consider the octad, say O_4 that contains x_1, x_2, x_5, x_6, x_7, which cuts both S_∞ as 2.2.2.2.0.0, by using π we can assume that it cuts the first four columns as 2.2.2.2.0.0. But it also cuts S_0 as 2.2.2.2.0.0, hence we get

x	x	x	x	
x	x	x	x	

Thus

$$S_2 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 1 & 2 & 2 \\ x & x & 1 & 1 & 2 & 2 \\ \hline 0 & 0 & 3 & 3 & 4 & 4 \\ 0 & 0 & 3 & 3 & 4 & 4 \\ \hline \end{array} \quad \text{is a sextet.}$$

Notice that $O_4 = Y_x \cup Y_1$. Now let O_5 contain x_1, x_2, x_3, x_5, x_7 such that $O_5 \neq O_4, O_3, O_2$ or O_1, and O_5 cuts S_∞, S_0 and S_1 as 3.1.1.1.1.1, so it must be

x	x	x	
x			x
x		x	
			x

or

x	x	x	
x			x
x			x
		x	

Figure 10

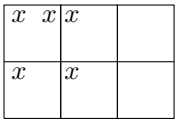
By using the permutation σ these are equivalent, we may assume

$$S_3 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 2 & 3 & 4 \\ x & 0 & 3 & 4 & 1 & 2 \\ \hline x & 0 & 4 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 & 4 & 3 \\ \hline \end{array} \quad \text{is a sextet.}$$

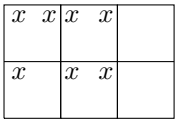
From figure 10

$$S_4 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 2 & 3 & 4 \\ x & 0 & 4 & 3 & 2 & 1 \\ \hline 0 & 0 & 2 & 1 & 4 & 3 \\ x & 0 & 3 & 4 & 1 & 2 \\ \hline \end{array} \quad \text{is a sextet.}$$

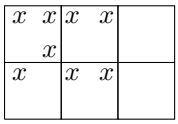
Now consider the octad containing the points



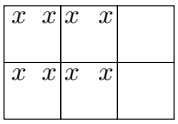
It must have further points in the second column and two points in one of the last three columns, but since it cuts S_∞, S_0 and S_1 as 2.2.2.2.0.0, we get



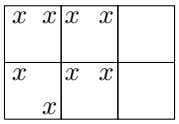
For the one point further that is in the second column we might have one of the following



(I)

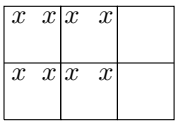


(II)



(III)

The first case (I) fails to cut S_2. (Because it cuts as 3.1.2.2.0.0 which is a contradiction with Lemma (5.11), wheras (II) and (III) are equivalent under ρ, so we might take (II) as our octad



Thus,

$$S_5 = \begin{array}{|cc|cc|cc|}\hline x & x & 1 & 1 & 3 & 3 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ \hline x & x & 1 & 1 & 3 & 3 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ \hline \end{array} \quad \text{is a sextet.}$$

Now we get $S_\infty, S_0, S_1, S_2, S_3, S_4, S_5$ and to obtain the 28 sextets remaining, we need the following Lemma.

5.15 Lemma

If every octad intersecting a given octad O in four points is known, then all octads follow by symmetric differencing.

Proof
Let O be the given octad and $x, y, z \in O$, which are distinct points. From figure 9 there are 21 octads containing x, y, z. But from Lemma (5.8) and Remark (5.6 and 5.7) any two octads intersect in $0, 2, 4$ or 8 points so the intersection must be in four points. Now there are $\binom{21}{2} = 210$ pairs, which are disjoint from x, y, z in 21 octads. Suppose $U_i, i = 1, 2, 3, 4$ are octads such that $x, y, z \in U_i, i = 1, 2, 3, 4$. if $U_1 + U_2 = U_3 + U_4$, then U_3 or U_4 must contain further two points from U_1, say U_3. so $|U_1 \bigcap U_3| = 5$. Hence $U_1 = U_3$ and this implies that $U_2 = U_4$. Therefore all 210 pairs are unique. Using figure 9 again the third line consists of all the disjoint octads from x, y, z. Hence we know every octad that is disjoint from O by three points.

5.16 Corollary

The set of all permutations of 24-element, Ω that preserve $S(5, 8, 24)$, and it has form quintuply transitive is a subgroup of symmetric group of 24-element, S_{24}. Moreover it has order $244,823,040$.

Proof
Notice that the set of all the permutations is a group and it is sharply transitive on sets which contain 7 points, say $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ where $x_1, x_2, x_3, x_4, x_5, x_6$ in the same octad, say O, whereas $x_7 \in \Omega \setminus O$. There are 24 ways of choosing x_1 from Ω, and 23 choices for choosing x_2, where there are $22, 21, 20$ choices for x_3, x_4, x_5, respectively. Now notice that $x_6 \in O$ and $|O| = 8$, hence there are three choices for x_6. Finally, there are 16 choices for choosing $x_7 \in \Omega \setminus O$. Therefore, $24 \times 23 \times 22 \times 21 \times 20 \times 3 \times 16 = 244,823,040$.

5.17 Definition

The 5-transitive group preserving $\mathscr{C}_8$ is called $M_{24} = \{\sigma \in S_{24} | O\sigma \in \mathscr{C}_8, \forall O \in \mathscr{C}_8\}$. Moreover, subgroups of M_{24} are M_{24-k}, where $(k < 5)$ which are fixed k-points.

5.18 Remark

Now we need to explain why we number the elements of Ω as $\infty, 0, 1, 2, ..., 22$. To see this suppose $\sigma \in M_{24}$ and $o(\sigma) = 23$, (notice that $|M_{24}| \diagup 23$). Now $\sigma : i \to i + 1$ $(mod\ 23)$ and it fixes ∞, or $\sigma = (\infty)(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22)$. Now we define another permutation of Ω, by $\gamma : i \to -1 \diagup i$. This implies that $\gamma = (0\ \infty)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18)$. To show that $\gamma \in M_{24}$, we need to check that $(S_i)\gamma$, $i = \infty, 0, 1, 2, 3, 4, 5$ is a sextet. Indeed they are sextets, hence $\gamma \in M_{24}$.

References

[1] F. Doherty, *History of finite simple groups*, pp40-42, 1997.

[2] L. Taslaman, *The Mathieu groups*, 2009.

[3] M. Grannell and T. Griggs, *An introduction to Steiner systems*, Mathematical Spectrum, 26 no.3, pp74-80, 1994.

[4] R. Curtis, *A new combinatorial approach to* M_{24}, Mathematical proceedings of the Cambridge Philosophical society, 79(1), pp25-42, 1976.