Sporadic Simple Groups

Simon Nickerson

May 2, 2002

Contents

1 Introduction

The Classification of Finite Simple Groups [Sol95] states that any finite simple group is one of the following:

- a cyclic group of prime order
- an alternating groups A_n (for $n \geq 5$)
- a classical linear group
- an exceptional or twisted group of Lie type
- one of 26 *sporadic simple groups.*

Five of the sporadic groups (M_{11}, M_{12}, M_{22}, M_{23} and M_{24}) were discovered by Mathieu in the 1860s. The other 21 groups were discovered (or at least predicted to exist) much more recently, in the period 1965–1974.

In this essay, we will mainly be concerned with the Mathieu groups. The largest of the Mathieu groups, M_{24}, acts on two exceptional structures: the $S(5,8,24)$ Steiner system $\mathcal{W}_{24}$ and the Golay code $\mathcal{C}_{24}$. We will examine these structures in detail, see how they are related, and show that they are unique up to isomorphism. The uniqueness proofs will give us some useful information about M_{24} and examining the structure of M_{24} will tell us about the other four Mathieu groups. We will be able to show that all five Mathieu groups are simple, and we will determine their orders.

The Mathieu groups are interesting not only because they are sporadic simple groups; they also have unusually high degrees of transitivity. We will see that M_{24} and M_{12} (another Mathieu group occurring as a subgroup of M_{24}) are 5-transitive on 24 and 12 points respectively.

In the final section, we will see how the Golay code allows us to construct another exceptional structure: the Leech lattice Λ. We will see three of the more modern sporadic groups (Co_1, Co_2 and Co_3) occurring in the group of automorphisms of Λ, and we will be able to determine their orders.

The main sources of information for this essay were [Con99], [Gri98], [Iva99], [Rot84] and [DM96]. Other sources used are listed in the bibliography.

2 The $S(5,8,24)$ Steiner system

An $S(t,k,v)$ *Steiner system* $(\Omega, \mathcal{S})$ consists of a finite set Ω, together with a set $\mathcal{S}$ of subsets of Ω satisfying the following conditions:

1. $|\Omega| = v$
2. Each $A \in \mathcal{S}$ has size k
3. Any set $B \subset \Omega$ of size t is contained in exactly one $A \in \mathcal{S}$

The elements of Ω are called *points*, and the elements of $\mathcal{S}$ are usually called *blocks* (although in the special case $t = 2$, they are sometimes called *lines*).

An *automorphism* of a Steiner system $(\Omega, \mathcal{S})$ is a permutation of Ω which induces a permutation of $\mathcal{S}$ (that is, blocks are sent to blocks). We will be especially interested in the automorphism group of an $S(5,8,24)$ Steiner system, as this group is the sporadic simple group M_{24}.

2.1 Basic properties of Steiner systems

We will need some basic results about an arbitrary $S(t,k,v)$ Steiner system $(\Omega,\mathcal{S})$.

Lemma 2.1.1 *The number of blocks containing a specified subset $B \subset \Omega$ of size $0 \le i \le t$ depends only on i, and is equal to:*

$$N_i := N(B) := \binom{v-i}{t-i} \Big/ \binom{k-i}{t-i} \tag{1}$$

Proof Given a set B of size i, there are $\binom{v-i}{t-i}$ t-subsets of Ω containing B. Each of these t-subsets is contained in a unique block of the Steiner system, but each block is counted once for each of its t-subsets containing B; there are $\binom{k-i}{t-i}$ such. This gives the required result. ■

Let us extend the definition by setting $N_i = 1$ for $t < i \le k$ (as this gives the number of blocks containing a set of size i, providing the set is contained in any block at all).

Lemma 2.1.2 *Suppose $A \subseteq B \subseteq \Omega$, with $|A| = i$, $|B| = j$. The number of blocks M satisfying $M \cap B = A$ is given by:*

$$N(A,B) := \sum_{A \subseteq C \subseteq B} (-1)^{|C-A|} N(C) \tag{2}$$

Moreover, if B is contained in some block, then $N(A,B)$ depends only on i and j (so we define $N_{i,j} := N(A,B)$ for any B contained in a block).

Proof We will prove (2) by induction on $t = |B - A| = j - i$ before showing that $N(A,B)$ only depends on i and j.

If $t = 0$, then $B = A$, and $N(A,B) = N(A,A) = N(A)$, so (2) is true for $t = 0$.

Now suppose that (2) holds for some $t \ge 0$. We want to show that it holds for $t+1$. Suppose $|B - A| = t + 1 \ge 1$. Then we can find an element $x \in B - A$. Define $B^- = B - \{x\}$ and $A^+ = A \cup \{x\}$. Then $|B^- - A| = |B - A^+| = t$, so by the induction hypothesis:

$$N(A,B^-) = \sum_{A \subseteq C \subseteq B^-} (-1)^{|C-A|} N(C) \tag{3}$$

and

$$N(A^+,B) = \sum_{A^+ \subseteq C \subseteq B} (-1)^{|C-A^+|} N(C) \tag{4}$$

Now, $N(A,B^-) = N(A,B) + N(A^+,B)$, for if L is a block, then $L \cap B^- = A$ if and only if either $L \cap B = A^+$ or $L \cap B = A$ (accordingly as $x \in L$). Moreover, if $A \subseteq C \subseteq B$ then either $A^+ \subseteq C \subseteq B$ or $A \subseteq C \subseteq B^-$ (accordingly as $x \in C$). Thus subtracting (4) from (3) gives:

$$N(A,B) = \sum_{A \subseteq C \subseteq B} (-1)^{|C-A|} N(C) \tag{5}$$

Equation (2) therefore holds by induction.

We now want to show that (2) depends only on i and j in the case that B is contained in a block L. If $A \subseteq C \subseteq B$, $N(C)$ is the same as $N_{|C|}$ (since we know that C is contained in the block L). The number of such subsets C of size l ($i \leq l \leq j$) is given by $\binom{j-i}{l-i}$. Hence:

$$N(A,B) = \sum_{l=i}^{j} \binom{j-i}{l-i} (-1)^{l-i} N_l \tag{6}$$

and the right hand side has no direct dependence on A or B. ■

Theorem 2.1.3 (Recurrence relation for $N_{i,j}$) *For $i \leq j < k$:*

$$N_{i,j} = N_{i,j+1} + N_{i+1,j+1} \tag{7}$$

Proof Let L_1 be a block and choose sets $A \subset B \subseteq L_1$ such that $|A| = i$, $|B| = j+1$. Choose $x \in B - A$, and let $A^+ = A \cup \{x\}$, $B^- = B - \{x\}$. As we remarked earlier,

$$N(A, B^-) = N(A,B) + N(A^+, B) \tag{8}$$

for if L is a block then $L \cap B^- = A$ if and only if either $L \cap B = A^+$ or $L \cap B = A$ (accordingly as $x \in L$). The result then follows from Lemma 2.1.2. ■

Lemma 2.1.1 allows us to calculate $N_i = N_{i,i}$ for all i, and the recurrence formula in Theorem 2.1.3 allows us to inductively calculate the other values of $N_{i,j}$. We can put these values in a table, called the *intersection table* for the Steiner system. Note that the intersection table only depends on the parameters (t,k,v) of the Steiner system. For example, all $S(5,8,24)$ Steiner systems have the intersection table given in Table 1.

$N_{i,j}$	$i = 0$	1	2	3	4	5	6	7	8
$j = 0$	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

Table 1: Intersection table for a $S(5,8,24)$ Steiner system

2.2 The projective plane of order 4

Let $(\Delta, \mathcal{L})$ be an $S(2, n+1, n^2+n+1)$ Steiner system: that is, Δ is a set of n^2+n+1 points, and $\mathcal{L}$ is a set of lines, each containing $n+1$ points, such that any two points are contained in a unique line. By Lemma 2.1.1, there are

$n+1$ lines containing each point and there are n^2+n+1 lines in total. Any two distinct lines intersect in a unique point: if L_1 and L_2 are distinct lines, then certainly $|L_1 \cap L_2| < 2$, and if $L_1 \cap L_2 = \emptyset$, then there are $(n+1)^2$ lines joining some point in L_1 to some point in L_2, and that is too many lines. So $(\Delta, \mathcal{L})$ obeys the axioms for a projective geometry, and we say that $(\Delta, \mathcal{L})$ is a *projective plane of order* n.

The reason why we are interested in projective planes is the following. Let $(\Omega, \mathcal{S})$ be an $S(5,8,24)$ Steiner system (postponing the question of existence for the time being). Let Y be any 3-subset of Ω, and consider the Steiner system $(\Delta, \mathcal{L})$ given by:

$$\Delta = \Omega - Y; \qquad \mathcal{L} = \{B - Y : B \in \mathcal{S}, Y \subseteq B\} \tag{9}$$

This is an $S(2,5,21)$ Steiner system (a projective plane of order 4), called the 3-point residual of $(\Omega, \mathcal{S})$ with respect to Y. In this section, we will prove:

Theorem 2.2.1 *There is a unique projective plane of order 4 (and hence, a unique $S(2,5,21)$ Steiner system) up to isomorphism.*

The easiest examples of finite projective planes are the *field planes.* Let q be a prime power, and let V be a 3-dimensional vector space over $\mathbb{F}_q$. Let Δ be the set of 1-dimensional subspaces of V. For each 2-dimensional subspace of V, let $B(W)$ be the set of 1-dimensional subspaces of W, and let $\mathcal{L}$ be the set of all the $B(W)$. Then $(\Delta, \mathcal{L})$ is a projective plane of order q, usually denoted by $PG(2,q)$. This settles the question of existence in Theorem 2.2.1. Note that for some n there exist projective planes of order n which are not field planes: see [AS68] for some examples. To prove the theorem, we will need to show that this is not the case for $n = 4$.

Points of $PG(2,q)$ are usually denoted by non-zero three-dimensional row vectors over $\mathbb{F}_q$ (with the understanding that two points are identical if their vectors are parallel). Lines of $PG(2,q)$ are represented by column vectors in a similar way. A point $\mathbf{p}$ lies on a line $\mathbf{l}$ if and only if $\mathbf{l}^\mathsf{T}\mathbf{p} = 0$

An *incidence matrix* $M = M_{ij}$ of a projective plane of order n is a matrix where rows represent lines L_i and columns represent points P_j (with $1 \le i,j \le n^2+n+1$) and the matrix entry M_{ij} is 1 if and only if the point P_j lies on the line L_i. The incidence matrix of $PG(2,4)$ (a projective plane of order 4) is given in Figure 1. Observe that each row and column contains exactly 5 '1's and any two rows and columns have exactly one '1' in common.

To prove Theorem 2.2.1, we will first consider a simpler Steiner system (motivated by the discussion in [DM96]). Let $(\Omega, \mathcal{S})$ be a projective plane of order n, and let L be one of the lines in $\mathcal{S}$. We can get another Steiner system by removing L and all of its points. Specifically, we let $\Omega_L = \Omega - L$ and $\mathcal{S}_L = \{B - L : B \in \mathcal{S} - \{L\}\}$. This is an $S(2,n,n^2)$ Steiner system: all the blocks contain n points, there are n^2 points in total, and any two points of Ω_L are contained in a block of $\mathcal{S}$ (which is not L), and hence, in exactly one block of $\mathcal{S}_L$. An $S(2,n,n^2)$ Steiner system is called a *affine plane of order* n.

Lemma 2.2.2 *For an affine plane of order n, if L is a line and P is a point not on L, then there is a unique line L' disjoint from L that contains P.*

$$\begin{bmatrix}
\cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 \\
\cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
1 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 \\
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot
\end{bmatrix}$$

Figure 1: Incidence matrix of $PG(2,4)$

Proof By Lemma 2.1.1, there are $N_1 = (n^2-1)/(n-1) = n+1$ lines going through P. Each line contains n points, so by the properties of the Steiner system, there are exactly n lines which intersect L and go through P. Thus there is exactly one line L' which goes through P but does not intersect L. ■

Lemma 2.2.3 *The lines of an affine plane of order n can be partitioned into $n+1$ classes, each containing n lines, such that the lines in each class are disjoint ("parallel").*

Proof Let L be a line on the affine plane $(\Omega, \mathcal{S})$. By Lemma 2.2.2, for each point P not on L, we can find a (unique) line $L(P)$ which contains P but is disjoint from L. Define:

$$\mathsf{S}(L) = \{L(P) : P \in \Omega - L\} \cup \{L\}$$

The lines in $\mathsf{S}(L)$ are disjoint from each other by the uniqueness of $L(P)$. Clearly each point is contained in some line in $\mathsf{S}(L)$, so $\mathsf{S}(L)$ is a partition of Ω into parallel lines. Thus $|\mathsf{S}(L)| = n$ (because each line has size n, and $|\Omega| = n^2$).

Note that $\mathsf{S}(L)$ is the only such partition of Ω into parallel lines that contains L (by the uniqueness of $L(P)$). Thus the set:

$$\mathsf{S} = \{\mathsf{S}(L) : L \in \mathcal{S}\}$$

is the required partition of $\mathcal{S}$ into $n+1$ classes of size n. ■

We will now concentrate on the case $n = 4$.

Theorem 2.2.4 *There is a unique affine plane of order 4 up to isomorphism.*

Proof Let $(\Omega, \mathcal{S})$ be an affine plane of order 4. By Lemma 2.2.3, we can find a partition of the 20 lines into 5 classes, each containing 4 parallel lines. Let two of the classes be $\{L_1, L_2, L_3, L_4\}$ and $\{M_1, M_2, M_3, M_4\}$, and call the remaining lines $K_1, \ldots, K_{12}$.

We now define a (4×12) matrix $T = (T_{ij})$ by the rule:

$$T_{ij} = k \quad \text{if } L_i \cap M_k \subset K_j \tag{10}$$

Observe:

1. This is well-defined. For any $1 \leq i, j \leq 4$, the set $L_i \cap K_j$ contains 1 point (it cannot contain more than 1, and if it contained 0, then L_i and K_j would be parallel, which cannot happen because they are in different classes). Let P be the unique point in $L_i \cap K_j$. Exactly one of the M_k contains P; thus there is exactly one value of k such that $L_i \cap M_k \subset K_j$.

2. The columns of the matrix T are a permutation of $1, 2, 3, 4$: if $T_{aj} = T_{bj} = k$ and $a \neq b$, then K_j and M_k are two distinct lines which contain a common 2-set $((L_a \cup L_b) \cap M_k)$, which is impossible.

3. T cannot contain a minor of the form $\begin{bmatrix} k_1 & & k_1 \\ k_2 & & k_2 \end{bmatrix}$. If it did, then we would have $T_{i_1 j} = k_1 = T_{i_1 j'}$ and $T_{i_2 j} = k_2 = T_{i_2 j'}$ for some i_1, i_2, j, j'. But then the distinct points $L_{i_1} \cap M_{k_1}$ and $L_{i_2} \cap M_{k_2}$ would both be contained in K_j and $K_{j'}$, which is impossible.

By reordering the L_i if necessary, we can suppose that the first column of T is $(1, 2, 3, 4)^{\mathsf{T}}$. In any column of T, the first two elements are different (by observation 2 above), and there are 12 ways of choosing the elements. By observation 3, no two columns can have the same top two elements. Thus all 12 combinations must occur, and by re-ordering the K_j if necessary, we can list them in lexicographic order:

$$T = \begin{bmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 & 4 & 4 & 4 \\ 2 & 3 & 4 & 1 & 3 & 4 & 1 & 2 & 4 & 1 & 2 & 3 \\ 3 & & & & & & & & & & & \\ 4 & & & & & & & & & & & \end{bmatrix} \tag{11}$$

By repeatedly using observations 2 and 3, it is a straightforward calculation to show that T must have the form:

$$T = \begin{bmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 & 4 & 4 & 4 \\ 2 & 3 & 4 & 1 & 3 & 4 & 1 & 2 & 4 & 1 & 2 & 3 \\ 3 & 4 & 2 & 4 & 1 & 3 & 2 & 4 & 1 & 3 & 1 & 2 \\ 4 & 2 & 3 & 3 & 4 & 1 & 4 & 1 & 2 & 2 & 3 & 1 \end{bmatrix} \tag{12}$$

But T completely determines the affine plane. ■

We are now ready to prove the uniqueness of the projective plane of order 4.

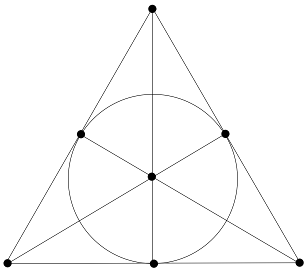

Figure 2: Fano plane

Proof of Theorem 2.2.1. Suppose $(\Omega_1, \mathcal{S}_1)$ and $(\Omega_2, \mathcal{S}_2)$ are projective planes of order 4. We will construct an isomorphism between them.

Choose lines $L_1 \in \mathcal{S}_1$, $L_2 \in \mathcal{S}_2$. Let $\mathcal{S}_i'$ denote the affine plane obtained by removing the line L_i from $\mathcal{S}_i$ $(i = 1, 2)$. $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are isomorphic by Theorem 2.2.4, so there is a bijection $\Omega_1 - L_1 \to \Omega_2 - L_2$.

Construct a bijection $L_1 \to L_2$ as follows. For $P \in L_1$, the lines containing P form a set of disjoint (parallel) lines in $\mathcal{S}_1'$. Such sets of parallel lines are preserved by the isomorphisms between affine planes, so there is a corresponding set of parallel lines in $\mathcal{S}_2'$. The corresponding lines in $\mathcal{S}_2$ must meet at a single point P' in L_2, so we map P to P'.

By combining these two maps, we get a bijection $\theta : \Omega_1 \to \Omega_2$. It is clear that θ sends the line L_1 to the line L_2. All the other lines in $\mathcal{S}_1$ comprise lines in $\mathcal{S}_1'$ together with a single point on L_1, and by construction of the map between L_1 and L_2 and the isomorphism between the affine planes, this line maps to a line in $\mathcal{S}_2$. Thus we have an isomorphism. ■

2.3 The geometry of $PG(2,4)$

In this section, we study some geometric properties of $PG(2,4)$ in preparation for the proof of the uniqueness of the $S(5,8,24)$ Steiner system. Firstly, we will need some terminology. A *Fano plane* is a projective plane of order 2 (see Figure 2). A set of points in a projective plane of order 4 is *independent* if no three of them are collinear. Indepedent 3-, 4- and 6-sets are known as *triangles*, *quadrangles* and *hyperovals* respectively. Triangles and quadrangles are sometimes *ordered*, in which case we have tuples (rather than sets) of points.

A *double-triangle* is a set of 4 points x_1, x_2, x_3, x_4 where x_1, x_2, x_3 collinear, and no other 3-subset collinear. An *ordered double-triangle* is the tuple equivalent.

Lemma 2.3.1 *1. $PG(2,4)$ contains 168 hyperovals, and every quadrangle is contained in a unique hyperoval.*

2. $PG(2,4)$ contains 360 Fano subplanes, and every quadrangle is contained in a unique Fano subplane.

3. The point set of a Fano subplane is the symmetric difference of a hyperoval and a line intersecting the hyperoval in two points.

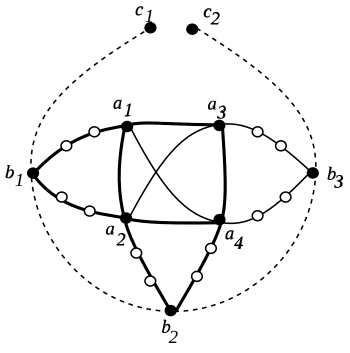

Figure 3: Some lines in $PG(2,4)$

Proof Consider the following construction. Let $A = \{a_1, a_2, a_3, a_4\}$ be any quadrangle (there are $21 \times 20 \times 16 \times 9/4! = 2520$ such). Each pair of points in A determines a line, and because A is an independent set, there are 6 such lines (call them A-lines). Two A-lines have a common point outside A if and only if they have no common point inside A; thus there are 3 points b_1, b_2, b_3 outside A which are intersections of A-lines (corresponding to partitions of A into 2-sets).

Each A-line contains 5 points, but each point of A is contained in 3 A-lines, and the points b_1, b_2, b_3 are contained in 2 A-lines each. Thus there are $6 \times 5 - 4 \times 2 - 3 \times 1 = 19$ points contained in some A-line. Call the remaining two points c_1 and c_2. The line going through c_1 and c_2 must be $\{b_1, b_2, b_3, c_1, c_2\}$ because it must intersect each of the lines $a_i a_j$ $(i \neq j)$ in exactly one point (in Figure 3).

1. The set $A' = A \cup \{c_1, c_2\}$ is a hyperoval, and by construction, it is the unique such containing A. So every quadrangle is contained in a unique hyperoval, Since every hyperoval contains $6 \times 5/2 = 15$ quadrangles, $PG(2,4)$ contains $2520/15 = 168$ hyperovals.

2. Any Fano subplane must contain a quadrangle A. Then it must also contain the A-lines, the intersections of the A-lines outside A (b_1, b_2, b_3) and the line through these intersection points ($\{b_1, b_2, b_3, c_1, c_2\}$). On the other hand, the points $\{a_1, \ldots, a_4, b_1, b_2, b_3\}$ and the lines joining them do in fact define a Fano subplane. So each quadrangle is contained in a unique Fano subplane, and the number of Fano subplanes is $2520/7 = 360$ (as each Fano subplane contains 7 quadrangles).

3. The point set $\{a_1, a_2, a_3, a_4, b_1, b_2, b_3\}$ of this (arbitrary) Fano subplane is the symmetric difference of the hyperoval $\{a_1, a_2, a_3, a_4, c_1, c_2\}$ and the line $\{b_1, b_2, b_3, c_1, c_2\}$ (which intersects the hyperoval in two places). ■

2.4 Connections between $PG(2,4)$ and $\mathcal{W}_{24}$

This section is based on [Iva99], [HP85] and [DM96], using the ideas of Lüneberg. We will show how a $S(5,8,24)$ Steiner system is related to the unique projective plane of order 4 ($PG(2,4)$). From our fairly detailed investigation of $PG(2,4)$, we will be able to deduce both the existence and uniqueness of the $S(5,8,24)$ Steiner system. This will lead to some useful information about its automorphism group M_{24}.

Suppose we have an $S(5,8,24)$ Steiner system $(\Omega, \mathcal{S})$, and fix a 3-element subset $Y = \{y_1, y_2, y_3\}$ of Ω. Then the blocks of $\mathcal{S}$ can be classified by the degree to which they intersect Y. We will call a block $B \in \mathcal{S}$ a *k-block* if $|B \cap Y| = k$.

Lemma 2.4.1 *$(\Omega, \mathcal{S})$ contains exactly 210 0-blocks, 360 1-blocks, 168 2-blocks and 21 3-blocks.*

Proof The number of k-blocks is the element $N_{k,3}$ on the fourth row of the intersection table for an $S(5,8,24)$ Steiner system (Table 1 on page 4) multiplied by $\binom{3}{k}$ (because the intersection of a k-block with Y could be any of the $\binom{3}{k}$ k-subsets of Y). ■

As before, we can get a projective plane $(\Delta, \mathcal{L})$ of order 4 by letting:

$$\Delta = \Omega - Y; \qquad \mathcal{L} = \{B - Y : B \in \mathcal{S}, B \supseteq Y\} \tag{13}$$

Theorem 2.4.2 (The k-block correspondence) *Let B be a block, and let $B' = B \cap \Delta$ be the restriction of B to the projective plane.*

- *If B is a 3-block, then B' is a line in $\mathcal{L}$.*
- *If B is a 2-block, then B' is a hyperoval in $\mathcal{L}$.*
- *If B is a 1-block, then B' is the point set of a Fano subplane in $\mathcal{L}$.*
- *If B is a 0-block, then B' is the symmetric difference of a pair of lines in $\mathcal{L}$.*

Conversely, we have:

- *If A is a line in $\mathcal{L}$, then A is contained in a 3-block.*
- *If A is a hyperoval in $\mathcal{L}$, then A is contained in a 2-block.*
- *If A is the point set of a Fano subplane in $\mathcal{L}$, then A is contained in a 1-block.*
- *If A is the symmetric difference of a pair of lines in $\mathcal{L}$, then A is contained in a 0-block.*

Proof Firstly, we will deal with the case where we are given a k-block $B \in \mathcal{S}$ ($k = 0, 1, 2, 3$).

- Case $k = 3$: this follows directly from equation (13) (the definition of $\mathcal{L}$).
- Case $k = 2$:

  B' is a set of 6 points in Δ. Suppose 3 points of B' lie on a line $L \in \mathcal{L}$. Then $L \cup Y$ is a block in $\mathcal{S}$ which intersects B in at least 5 points. Since $(\Omega, \mathcal{S})$ is a $S(5,8,24)$ Steiner system, we must have $B = L \cup Y$. But $|B \cap Y| = 2$, a contradiction. So no three points of B' are collinear, and hence B' is a hyperoval.

- Case $k=1$:

  B' is a set of 7 points in Δ. Let $\mathcal{L}'$ be the set of lines in $\mathcal{L}$ which meet B' in at least 2 points. We want to show that $(B', \mathcal{L}')$ is a Fano subplane, i.e. a $S(2,3,7)$ Steiner system. It is clear that any two points of B' are contained in exactly one line in $\mathcal{L}'$, so we only need to show that any line of $\mathcal{L}'$ meets B' in exactly 3 points. For any $L \in \mathcal{L}'$, $L \cup Y$ is a block, and any two distinct blocks in $\mathcal{S}$ intersect in 0, 2 or 4 points (by Table 1 on 4). Thus $|B' \cap L|$ is either 1 or 3. But by definition of $\mathcal{L}'$, we cannot have $|B' \cap L| = 1$. Thus $|B' \cap L| = 3$, so B' is the point set of a Fano subplane.

- Case $k=0$:

  B is an 8-subset of Δ. Consider a point $P \in B$. P is contained in 5 lines $L_1(P), \ldots L_5(P)$ in $\mathcal{L}$. Each of these lines $L_i(P)$ meets B in 0, 2 or 4 points (because $L_i(P) \cup Y$ is a block and $B \cap Y = \emptyset$), and clearly it cannot be 0 points, as $P \in L_i(P) \cap B$. Thus any line containing P meets B in 2 or 4 points.

  There is a unique line in $\mathcal{L}$ going through any two points in Δ, so

  $$\{L_i(P) \cap B - \{P\} : 1 \leq i \leq 5\}$$

  is a partition of $B - \{P\}$. Therefore, exactly one of the lines, say $L_1(P)$, meets B in 4 points, and the other 4 lines $(L_2(P), \ldots, L_5(P))$ meet B in 2 points.

  Now, let Q be any point in $B - L_1(P)$. By the above argument, there is a unique line $L_1(Q)$ containing Q such that $|L_1(Q) \cap B| = 4$.

  Clearly $L_1(P) \neq L_1(Q)$, so they must meet at a single point R. This point R is on two lines, each containing 4 points of B, but if $R \in B$, then there can only be one such line (namely $L_1(R)$). So $R \notin B$, and hence by counting points, $L_1(P) \bigtriangleup L_1(Q) = B$. Thus B is the symmetric difference of two lines.

Conversely, we will show that the correspondence is 1-1 by counting each of the sets.

- Case $k=3$. There are 21 lines in $\mathcal{L}$ and 21 3-blocks.
- Case $k=2$. There are 168 hyperovals in $\mathcal{L}$ and 168 2-blocks.
- Case $k=1$. There are 360 Fano subplanes in $\mathcal{L}$ and 360 1-blocks.
- Case $k=0$. There are $21 \times 20/2 = 210$ unordered pairs of lines in Δ, and different pairs of lines give rise to different symmetric differences. Thus there are 210 sets which are the symmetric difference of two lines of $\mathcal{L}$, and there are 210 0-blocks. ■

The correspondence indicates that we should expect hyperovals and Fano subplanes to be important when trying to extend $PG(2,4)$ to an $S(5,8,24)$ Steiner system.

Define the following sets for $i = 1,2,3$.

$$\mathsf{H}_i = \{\text{ovals } H \in \mathcal{L} : y_i \notin \text{the unique block containing } H\} \tag{14}$$

$$\mathsf{F}_i = \{\text{Fano subplane } F \in \mathcal{L} : y_i \in \text{the unique block containing } F\} \tag{15}$$

We call two hyperovals (or two Fano subplanes) *equivalent* if they are both in H_i (or both in F_i) for some i. This is an equivalence relation, because the sets H_i partition the set of hyperovals, and the sets F_i partition the set of Fano subplanes. In fact, two hyperovals (or Fano subplanes) are equivalent if and only the blocks containing them have the same intersection with Y.

From the intersection table (Table 1 on page 4) and the k-block correspondence (Theorem 2.4.2), we know that each H_i contains 56 hyperovals and each F_i contains 120 Fano subplanes.

The next two lemmas are easy but highly significant, as they show that the classes of hyperovals and Fano subplanes are dependent on the geometry of $PG(2,4)$ rather than the geometry of the $S(5,8,24)$ Steiner system. This observation will be crucial when we prove the uniqueness of the $S(5,8,24)$ Steiner system.

Lemma 2.4.3 *Two hyperovals H_1 and H_2 are equivalent if and only if $|H_1 \cap H_2|$ is even.*

Proof Let O_i be the unique block containing H_i ($i = 1,2$): such exists by Theorem 2.4.2). Then $H_1 \cap H_2 = O_1 \cap O_2 - Y$.

Suppose H_1 and H_2 are equivalent. Then $|H_1 \cap H_2| = |O_1 \cap O_2| - 2$, which is even by the intersection triangle for an $S(5,8,24)$ Steiner system.

Conversely, suppose $|H_1 \cap H_2|$ is even. Then $|O_1 \cap O_2 - Y|$ is even, and since $|O_1 \cap O_2|$ is even (by the intersection table), so is $|O_1 \cap O_2 \cap Y|$. But O_1 and O_2 must have at least one point of Y in common (because $|Y| = 3$), so $|O_1 \cap O_2 \cap Y| = 2$. Thus $O_1 \cap Y = O_2 \cap Y$, i.e. H_1 and H_2 are equivalent. ■

Lemma 2.4.4 *Two Fano subplanes F_1 and F_2 are equivalent if and only if $|F_1 \cap F_2|$ is odd.*

Proof This proof is virtually the same as that of Lemma 2.4.3. Let O_i be the unique block containing F_i ($i = 1,2$: such exists by Theorem 2.4.2). So $F_1 \cap F_2 = O_1 \cap O_2 - Y$.

Suppose F_1 and F_2 are equivalent. Then $|F_1 \cap F_2| = |O_1 \cap O_2| - 1$, whence $|F_1 \cap F_2|$ is odd.

Conversely, suppose $|F_1 \cap F_2|$ is odd. Then $|O_1 \cap O_2 \cap Y|$ is odd. The size cannot be 3, so it must be 1. Thus F_1 and F_2 are equivalent. ■

Theorem 2.4.5 *An $S(5,8,24)$ Steiner system (if it exists) is unique up to isomorphism.*

Proof Any $S(5,8,24)$ Steiner system must be built up from a projective plane of order 4 (unique up to isomorphism) with blocks as described above. By Theorem 2.4.2 and Lemmas 2.4.3 and 2.4.4, the nature of these blocks is determined (except for relabelling of the three extra points) by the geometry of $PG(2,4)$, so there is essentially only one way to proceed. Thus any two $S(5,8,24)$ Steiner systems are isomorphic. ■

We have still not shown that an $S(5,8,24)$ Steiner system exists at all, but we know quite a lot about what such a Steiner system must look like.

2.5 Groups acting on $PG(2,4)$

We have seen that, given an $S(5,8,24)$ Steiner system, the hyperovals and Fano subplanes in a residual projective plane of order 4 fall into 3 classes. In this section, we will see how this can occur without reference to an $S(5,8,24)$ Steiner system: it turns out that the 3 classes are orbits under the action of the group $PSL_3(4)$.

Since there is only one projective plane of order 4, we will use the standard co-ordinate representation of the field plane $PG(2,4)$.

The group $GL_3(4)$ of non-singular 3×3 matrices over $\mathbb{F}_4$ acts on $PG(2,4)$ in the obvious fashion. The action is not faithful; to get a faithful group action, we take instead the group $PGL_3(4) \cong GL_3(4)/Z$, where $Z = \{kI : k \in \mathbb{F}_4^*\}$. $PGL_3(4)$ has a subgroup $PSL_3(4)$ obtained by taking only matrices of determinant 1. Since $x^3 = 1$ for all $x \in \mathbb{F}_4^*$, we have that $PSL_3(4) \cong SL_3(4)/Z$.

Lemma 2.5.1 *For any prime power q, $PGL_3(q)$ is transitive on ordered quadrangles in $PG(2,q)$.*

Proof Let $Q = (P_1, P_2, P_3, P_4)$ be an ordered quadrangle in $PG(2,q)$, where $P_i = [(p_{i1}, p_{i2}, p_{i3})]$. It is sufficient to show that element of $PGL_3(q)$ sends the standard quadrangle $S_1 = \langle(1,0,0)\rangle$, $S_2 = \langle(0,1,0)\rangle$, $S_3 = \langle(0,0,1)\rangle$, $S_4 = \langle(1,1,1)\rangle$ to Q.

The matrix

$$A = \begin{bmatrix} p_{11} & p_{21} & p_{31} \\ p_{12} & p_{22} & p_{32} \\ p_{13} & p_{23} & p_{33} \end{bmatrix}$$

is non-singular, for if there were a vector $\mathbf{x} \neq \mathbf{0}$ such that $A\mathbf{x} = 0$, then $\langle \mathbf{x} \rangle$ would represent a line containing P_1, P_2 and P_3, which is impossible as Q is an (ordered) quadrangle.

Since A is non-singular, there exists a vector $\mathbf{y} = (y_1, y_2, y_3)^{\mathsf{T}}$ such that $A\mathbf{y} = (p_{41}, p_{42}, p_{43})$. If any of the y_i were zero, then three points of the standard quadrangle would lie in a two-dimensional subspace of $\mathbb{F}_q^3$, which is not the case. Therefore all the y_i are non-zero. Thus the image of the non-singular matrix:

$$B = \begin{bmatrix} y_1 p_{11} & y_2 p_{21} & y_3 p_{31} \\ y_1 p_{12} & y_2 p_{22} & y_3 p_{32} \\ y_1 p_{13} & y_2 p_{23} & y_3 p_{33} \end{bmatrix}$$

in $PGL_3(4)$ sends S_i to P_i. ■

Lemma 2.5.2 *$PSL_3(4)$ has 3 equally-sized orbits on quadrangles.*

Proof Consider the standard quadrangle

$$Q = \{\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(0,0,1)\rangle, \langle(1,1,1)\rangle\};$$

there is no real loss of generality here.

We can consider Q as a quadrangle in either $PG(2,4)$ or $PG(2,2)$. Let K_4 and K_2 denote the stabilizers of Q in $PGL_3(4)$ and $PGL_3(2)$ respectively. It is clear that $K_4 \geq K_2$. Note that by Lemma 2.5.1, $PGL_3(4)$ is transitive on ordered quadrangles in $PG(2,4)$, so K_4 is 4-transitive on the points of Q. Since the only element of $PGL_3(4)$ that fixes an ordered quadrangle is the identity, we see $K_4 \cong S_4$. By exactly the same argument, we get $K_2 \cong S_4$, and so $K_4 = K_2$. But note that all matrices in $GL_3(2)$ have determinant 1 (because we are working over $\mathbb{F}_2$), so we must have $K_4 \subseteq PSL_3(4)$. In other words, the stabilizer of Q in $PSL_3(4)$ is K_4.

So, by the Orbit-Stabilizer Theorem, the size of the orbit of Q under $PSL_3(4)$ is $|PSL_3(4)|/|K_4| = 20160/24 = 840$. But there are 3 times as many (2520) in the whole of $PG(2,4)$. ■

Lemma 2.5.3 *If H is a hyperoval, then all the quadrangles contained in H are in the same $PSL_3(4)$-orbit.*

Proof Let K be the stabilizer of the hyperoval H in $PGL_3(4)$. $PGL_3(4)$ (and therefore K) is transitive on the ordered quadrangles contained in H (there are $6 \cdot 5 \cdot 4 \cdot 3$ of them), and the subgroup that fixes an ordered quadrangle is trivial. Every quadrangle is in a unique oval, so K is 4-transitive on the 6 points of H with order $6 \cdot 5 \cdot 4 \cdot 3$. So K must act on H like A_6. Now $K' = PSL_3(4) \cap K$ is a normal subgroup of K, but $K \cong A_6$ is simple, so $K' = K$ or $K = 1$.

If $K' = 1$, then only the identity in $PSL_3(4)$ fixes H, so H has $|PSL_3(4)| = 20160$ images under $PSL_3(4)$, which is impossible, as there are only 168 hyperovals. Thus $K' = K$, so $PSL_3(4)$ is transitive on the quadrangles contained in H. ■

Lemma 2.5.4 *If F is a Fano subplane, then all the quadrangles in F are in the same $PSL_3(4)$-orbit.*

Proof This is basically the same proof as for Lemma 2.5.3, except that the subgroup fixing a Fano subplane is isomorphic to the simple group $PGL_3(2)$. ■

Lemma 2.5.5 *$PSL_3(4)$ is transitive on ordered triangles and ordered double-triangles.*

Proof The stabilizer of the ordered triangle

$$\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(0,0,1)\rangle$$

in $PSL_3(4)$ is induced by the subgroup of diagonal matrices in $SL_3(4)$. This stabilizer has size 3, so the size of the orbit under $PSL_3(4)$ is $20160/3 = 6720 = 21 \times 20 \times 16$, which is the number of ordered triangles.

The stabilizer of the ordered double-triangle

$$\langle(1,0,0)\rangle, \langle(1,1,0)\rangle, \langle(0,1,0)\rangle, \langle(0,0,1)\rangle$$

in $PSL_3(4)$ is trivial, so the size of the orbit is $20160/1 = 21 \times 20 \times 3 \times 16$, which is the number of ordered double-triangles. ■

Lemma 2.5.6 *$PSL_3(4)$ has 3 orbits on hyperovals, and each triangle is in exactly one hyperoval of each orbit.*

Proof We have shown that there are 3 orbits for quadrangles, and all the quadrangles for a hyperoval are in the same orbit. So there are 3 orbits for hyperovals. Since $PSL_3(4)$ is transitive on triangles, each triangle is in at least one hyperoval for each orbit. But each triangle is contained in 9 quadrangles, each quadrangle is contained in exactly one hyperoval, and each hyperoval contains 3 quadrangles containing a particular triangle. Thus each triangle is contained in exactly 3 hyperovals, and so exactly one from each orbit. ■

Lemma 2.5.7 *$PSL_3(4)$ has 3 orbits on Fano subplanes, and each double triangle is one Fano subplane of each orbit.*

Proof This is basically the same as Lemma 2.5.6. We can see that there are 3 orbits for Fano subplanes, and it is possible to show that each double triangle is contained in exactly three Fano subplanes. ■

2.6 Construction of a $S(5,8,24)$ Steiner system

We now have enough information to construct an $S(5,8,24)$ Steiner system.

Take a projective plane $(\Delta, \mathcal{L})$ of order 4. The set of points of our new Steiner system is $\Omega = \Delta \cup Y$, where $Y = \{\infty_1, \infty_2, \infty_3\}$ and $\Delta \cap Y = \emptyset$.

Let the 3 $PSL_3(4)$-orbits of quadrangles be denoted Q_i for $1 \leq i \leq 3$. By Lemmas 2.5.3 and 2.5.4, we can define H_i to be the set of those hyperovals whose quadrangles are in Q_i, and similarly, F_i to be the set of those Fano subplanes whose quadrangles are in Q_i.

Then, motivated by the k-block correspondence, we define the blocks of our new Steiner system to be all sets of the following four types:

- $L \cup Y$ for lines $L \in \mathcal{L}$ (3-blocks).
- $H \cup Y - \{\infty_i\}$ for hyperovals $H \in \mathsf{H}_i$, $i = 1,2,3$ (2-blocks).
- $F \cup \{\infty_i\}$ for Fano subplanes $F \in \mathsf{F}_i$, $i = 1,2,3$ (1-blocks).
- $L \bigtriangleup L'$ for distinct lines $L, L' \in \mathcal{L}$ (0-blocks).

Let $\mathcal{S}$ be the set of blocks.

Theorem 2.6.1 *$(\Omega, \mathcal{S})$ is an $S(5,8,24)$ Steiner system.*

Proof There are 24 points in Ω, and each block of $\mathcal{S}$ contains 8 points. We need to show that any 5-subset F of Ω is contained in exactly one block. We will start by showing that F is contained in some block B.

Let $Y' = F \cap Y$, $P' = F \cap \Delta$. Let $L \in \mathcal{L}$ be a line of maximal intersection with P' (there may be several such lines).

Without loss of generality, we may suppose that the points of Y' are ∞_i $(1 \leq i \leq |Y'|)$. There are four cases to consider:

1. $|Y'| = 3$, $Y' = \{\infty_1, \infty_2, \infty_3\}, |P'| = 2$

   We have $P' \subset L$, so take $B = Y \cup L$.

2. $|Y'| = 2$, $Y' = \{\infty_1, \infty_2\}, |P'| = 3$

- If $|P' \cap L| = 3$, then $P' \subseteq L$, so take $B = Y \cup L$.
- Otherwise, P' is a triangle. By Lemma 2.5.6, there is a hyperoval $H \in \mathsf{H}_3$ containing this triangle. Then take $B = H \cup \{\infty_1, \infty_2\}$.

3. $|Y'| = 1$, $Y' = \{\infty_1\}, |P'| = 4$

   - If $|P' \cap L| = 4$, then $P' \subseteq L$, so take $B = Y \cup L$.
   - If $|P' \cap L| = 3$, then P' is a double triangle. By Lemma 2.5.7, there is a Fano subplane $F \in \mathsf{F}_1$ containing this double triangle. Then take $B = F \cup \{\infty_1\}$.
   - Otherwise, no three of the P_i are collinear, i.e. the P_i form a quadrangle Q. If $Q \in \mathsf{Q}_1$, then Q is in a Fano subplane $F \in \mathsf{F}_1$, and we can take $B = F \cup \{\infty_1\}$. If Q is in one of the other $PSL_3(4)$ orbits (say Q_2), then Q is in a unique hyperoval $H \in \mathsf{H}_2$, and we can take $B = H \cup \{\infty_1, \infty_3\}$.

4. $|Y'| = 0$, $Y' = \emptyset$, $|P'| = 5$

   Write $P' = \{P_1, \ldots, P_5\}$, with the points on $P' \cap L$ listed first.

   - If $|P' \cap L| = 5$, then $P' \subseteq L$, so take $B = Y \cup L$.
   - If $|P' \cap L| = 4$, then let P_5' be the fifth point on L (i.e. $L = \{P_1, \ldots, P_4, P_5'\}$), and let M be the line between P_5 and P_5'. Then take $B = L \triangle M$.
   - If $|P' \cap L| = 3$, then let M be the line joining P_4 and P_5. If L and M meet at a point in P', say P_1, then $\{P_2, P_3, P_4, P_5\}$ is a quadrangle, contained in a Fano subplane $F \in \mathsf{F}_i$, and we can take $B = F \cup \{\infty_i\}$. Otherwise, L and M meet at a point not in P'; in which case, take $B = L \triangle M$.
   - Otherwise, no three of the P_i are collinear. Then there is a hyperoval $H \in \mathsf{H}_i$ (for some $1 \leq i \leq 3$) containing P'. Then take $B = H \cup Y - \{\infty_i\}$.

So every 5-set is contained in some block. On the other hand, there are $21+168+360+(21\times 20/2) = 759$ blocks in $\mathcal{S}$, so the number of 5-sets contained in some block (counting multiplicity) is $759 \times \binom{8}{5} = 42504$. Since this is precisely $\binom{24}{5}$ (the number of 5-sets in Ω), we must have counted each 5-set exactly once. It follows that each every 5-set is contained in a unique block of $\mathcal{S}$. ■

3 The Golay code

In this section, we will introduce another one of the main characters in our sory: the extended binary Golay code.

3.1 Linear codes

We will start by introducing some terminology from coding theory. Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. A *q-ary linear code of length n* is a vector subspace of $\mathbb{F}_q^n$. The dimension of the subspace is the *rank* of the code. Vectors in the subspace are called *codewords*. Individual co-ordinates in a codeword are called the *letters* of the codeword.

The *weight* $w(x)$ of a codeword x is the number of non-zero letters in the codeword, and the *Hamming distance* $d(x, y)$ between two codewords x and y is $w(x-y)$. The *minimum distance* or *minimum weight* $d(\mathcal{X})$ of a linear code $\mathcal{X}$ is given by the smallest non-zero value of $w(x)$ for a codeword $x \in \mathcal{X}$.

A q-ary linear code of length n, rank k and minimum weight d is said to be a *q-ary $[n, k, d]$ code*, and n, k, d are said to be *parameters* of the code. There are restrictions on the code parameters. By a sphere-packing argument, Hamming showed that the following inequality holds for a q-ary $[n, k, d]$ code:

$$\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor} \binom{n}{i} \leq q^{n-k} \tag{16}$$

A code which attains equality in (16) is said to be a *perfect code*. Very few perfect codes exist. Aside from trivial examples, the only perfect codes are the so-called *Hamming codes* with parameters $n = (q^l - 1)/(q-1)$, $k = n - l$, $d = 3$ for integers $l \geq 3$, $q \geq 2$, some other codes with the same parameters as the Hamming codes, the binary [23, 11, 7] Golay code $\mathcal{C}_{23}$ and a ternary [11, 6, 5] code $\mathcal{C}_{11}$. (This result is proved in [MS77] chapter 6, section 10.) In the next section, we will construct a binary [24,12,8] code $\mathcal{C}_{24}$; removing the last letter from each codeword of $\mathcal{C}_{24}$ gives us $\mathcal{C}_{23}$.

3.2 Construction of the Golay code $\mathcal{C}_{24}$

Let P be the projective line over the finite field $\mathbb{F}_{23}$. We will make the identification $P = \mathbb{F}_{23} \cup \{\infty\}$, where ∞ obeys the usual rules ($\infty \times a = \infty$, $a/0 = \infty$ and $a/\infty = 0$ for $a \neq 0$, and $a + \infty = \infty$ for all $a \in P$).

We denote the set of subsets of P by $\mathcal{P}(P)$. This is a $\mathbb{F}_2$-vector space with addition represented by symmetric difference and scalar multiplication by the rules $1A = A, 0A = \emptyset$ for $A \subseteq P$. We will construct $\mathcal{C}_{24}$ as a subspace of $\mathcal{P}(P)$.

The quadratic residues of $\mathbb{F}_{23}$ are given by the elements of:

$$Q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \tag{17}$$

and the quadratic non-residues are given by the elements of:

$$N = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\} \tag{18}$$

For $a \in \mathbb{F}_{23}$, define:

$$N_a = \{n + a | n \in N\} \cup \{a\} = (N \cup \{0\}) + a \tag{19}$$

and let $\mathbb{B}$ be the set of all the N_a, together with P. Let $\mathcal{C}_{24}$ be the code generated by the sets of $\mathbb{B}$.

We are aiming to prove:

Theorem 3.2.1 *The extended binary Golay code* $\mathcal{C}_{24}$ *is a binary linear* $[24, 12, 8]$ *code.*

To do this, we work with a group acting on $\mathcal{C}_{24}$. Let M be the group of Möbius transformations:

$$x \mapsto \frac{ax+b}{cx+d}, \qquad ad - bc \in Q$$

on P. M is isomorphic to the finite group $PSL_2(23)$. We pick out three elements of M:

- $t : x \mapsto x + 1$,

  $(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22)(\infty)$

- $s : x \mapsto 2x$

  $(0)(\infty)(1\ 2\ 4\ 8\ 16\ 9\ 18\ 13\ 3\ 6\ 12)(5\ 10\ 20\ 17\ 11\ 22\ 21\ 19\ 15\ 7\ 14)$

- $\tau : x \mapsto -1/x$

  $(0\infty)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18)$

Lemma 3.2.2 *For the group* M *defined above:*

1. *M acts transitively on the 2-subsets of P.*

2. *M acts transitively on the 3-subsets of P.*

3. *M has order* $24 \times 23 \times 11$.

4. *M is generated by the elements s, t, τ.*

Proof

1. Firstly we show that the point-stabilizer M_∞ of ∞ acts transitively on the 2-subsets of $\mathbb{F}_{23}$. Suppose we have a, b, c, d in $\mathbb{F}_{23}$ ($a \neq b$, $c \neq d$) and we want to find an element of M_∞ which maps $\{a, b\}$ to $\{c, d\}$. Assume that $(c - d)/(a - b) \in Q$; if not, then swap a and b. The group M_∞ consists of transformations $x \mapsto qx + d$ with $q \in Q$, $d \in \mathbb{F}_{23}$, so we want to find $q \in Q$, $r \in \mathbb{F}_{23}$ such that

   $$aq + r = c; \qquad bq + r = d$$

   Subtracting the equations gives $q = (c - d)/(a - b) \in Q$. We then set $r = c - aq$ and it is easily seen that $x \mapsto qx + d$ maps $\{a, b\}$ to $\{c, d\}$.

   Since τ does not fix ∞, we see that M acts transitively on the 2-subsets of P.

2. Let M act on the 3-subsets of P. Any orbit under this action contains a subset $\{0, \infty, a\}$ with $a \in \mathbb{F}_{23}$, because M is transitive on the 2-subsets of P. Under the action of $\langle s \rangle$, this subset maps to 11 other subsets of the same form, accordingly as $a \in Q$ or $a \in N$. Thus there are at most 2 orbits under the action of M on the 3-subsets of P. But the element τ stabilises $\{0, \infty\}$ and transposes Q and N, so there is only one orbit.

3. Let $T = \langle t \rangle$, $S = \langle s \rangle$. T is a cyclic group of order 23 acting regularly on $\mathbb{F}_{23}$, and S is a cyclic group of order 11 acting on Q (or N).

   T and S are clearly subgroups of M_∞, and in fact $T \triangleleft M_\infty$. Indeed, if $g : x \mapsto qx + d$ then for any n:

   $$g^{-1}t^n g(x) = (((qx + d) + n) - d)/q = x + n/q$$

   so $g^{-1}t^n g \in T$. Moreover, $S = M_{(\infty 0)}$, the elementwise stabilizer of 0 and ∞. Since T is a normal subgroup of M_∞ acting regularly on $\mathbb{F}_{23}$, we deduce that M_∞ is a split extension (a semi-direct product) of T by $M_{(\infty 0)} = S$. In particular, $|M_\infty| = |T||S| = 23 \times 11$.

   Since M is transitive on P, by the Orbit-Stabilizer Theorem:

   $$|M| = |M_\infty||\infty^M| = 23 \times 11 \times 24$$

4. We have proved that M_∞ is the semi-direct product of T by S, so M_∞ is generated by s and t. By adding the element τ we get a group which is transitive on the 2-subsets of P with order $23 \times 11 \times 24$ as above. So $\langle s, t, \tau \rangle$ is a subgroup of M with the same order as M, which proves that M is generated by s, t and τ. ■

Lemma 3.2.3 *For $a \in \mathbb{F}_{23}$, $N_a t = N_{a+1}$ and $N_a s = N_{2a}$.*

Proof The statement for t is clear. Since 2 is a quadratic residue in $\mathbb{F}_{23}$, $N_0 s = N_0$, and so $N_a s = (N_0 + a)s = N_0 + 2a = N_{2a}$. ■

Lemma 3.2.4 *For any distinct $a, b \in \mathbb{F}_{23}$, $|N_a \cap N_b| = 6$. In particular, the intersection of any two elements of $\mathbb{B}$ is even.*

Proof By Lemma 3.2.3, the actions of s and t on $\{N_a | a \in \mathbb{F}_{23}\}$ mimic their actions on $\mathbb{F}_{23}$. In particular, by transitivity on 2-subsets, we can find an element $g \in M$ such that $\{N_a, N_b\}g = \{N_0, N_1\}$, and in particular, $(N_a \cap N_b)g = N_0 \cap N_1$. Now:

$$N_0 = \{0, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

and

$$N_1 = \{0, 1, 6, 8, 11, 12, 15, 16, 18, 20, 21, 22\}$$

so

$$N_0 \cap N_1 = \{0, 11, 15, 20, 21, 22\}$$

Thus $|N_a \cap N_b| = 6$. ■

Theorem 3.2.5 *$\mathcal{C}_{24}$ is preserved by the group M.*

Proof Because M is generated by s, t and τ, and $\mathcal{C}_{24}$ is generated by P and $\{N_a | a \in \mathbb{F}_{23}\}$, it is sufficient to show that s, t and τ send P and each N_a to elements of $\mathcal{C}_{24}$. It is obvious that nothing happens to P, and Lemma 3.2.3 has dealt with the actions of s and t. Thus it only remains to see how τ acts on N_a for $a \in \mathbb{F}_{23}$.

The elements of $N_a\tau$ are $m = \frac{-1}{n+a}$ for $n \in N$. We have:

$$m + \frac{1}{a} = \frac{n}{(n+a)a} \tag{20}$$

- Suppose $a \in Q$. Then $m \in N_{-1/a}$ if and only if $m + \frac{1}{a} \in N_0$, if and only if $\frac{n}{n+a} \in N_0$, if and only if $m \in N_0$. So $N_a\tau \subseteq N_{-1/a} \bigtriangleup N_0 \bigtriangleup P$. But the two sets both contain 12 elements, so must be equal.
- Suppose $a \in N$. Then $m \in N_{-1/a}$ if and only if $m \notin N_0$. So $N_a\tau \subseteq N_{-1/a} \bigtriangleup N_0$. But the two sets both contain 12 elements, so must be equal.
- Otherwise, $a = 0$, and it is clear that $N_0\tau = P \bigtriangleup N_0 \in \mathcal{C}_{24}$.

So $N_a\tau \in \mathcal{C}_{24}$. ■

We are now ready to prove that $\mathcal{C}_{24}$ is a [24, 12, 8] code.

Proof of 3.2.1. It is clear that $\mathcal{C}_{24}$ has length 24; we need to show (1) that it has rank 12, and (2) that it has minimum distance 8.

1. The cyclic group T of order 23 acts on the quotient $Q = \mathcal{C}_{24}/\langle P\rangle$. All the orbits of this action have size 23, except the orbit of the zero vector (which has size 1), so 23 divides $|Q| - 1$. But $Q = 2^m$ for some m, and the least m for which 23 divides $2^m - 1$ is given by $m = 11$. So the rank of $\mathcal{C}_{24}$ is at least $m + 1 = 12$.

   On the other hand, $\mathcal{C}_{24}$ cannot have rank greater than 12. By Lemma 3.2.4, the intersection of any two elements of $\mathbb{B}$ is even. We introduce a non-singular inner product $\langle *, * \rangle : \mathbb{F}_2^{24} \times \mathbb{F}_2^{24} \to \mathbb{F}_2$:

$$\langle A, B\rangle = \begin{cases} 0 & \text{if } |A \cap B| \text{ is even} \\ 1 & \text{if } |A \cap B| \text{ is odd} \end{cases} \tag{21}$$

   With respect to this inner product, $\mathcal{C}_{24}$ is contained in its own dual, and so cannot have rank greater than 12. (This also implies that all codewords in $\mathcal{C}_{24}$ have even weight).

   So the rank of $\mathcal{C}_{24}$ is exactly 12.

2. The minimum distance of $\mathcal{C}_{24}$ is at most 8, because $N_0 \in \mathcal{C}_{24}$ has weight 8. To show that the minimum distance is at least 8, it suffices to show that $\mathcal{C}_{24}$ contains no non-zero words of weight less than 8. In fact, it suffices to show that $\mathcal{C}_{24}$ contains no words of weight 2, 4 or 6, because we showed above that all words in $\mathcal{C}_{24}$ have even weight.

   - $\mathcal{C}_{24}$ contains no word of weight 2.

     Suppose $\mathcal{C}_{24}$ contained a set of size 2. The group M is transitive on the 2-subsets of P, and by Theorem 3.2.5, M preserves $\mathcal{C}_{24}$. So

$\mathcal{C}_{24}$ contains all 2-subsets of P, and hence all the even subsets of P (there are 2^{23} of them). But the dimension of $\mathcal{C}_{24}$ is only 12, so this is impossible.

- $\mathcal{C}_{24}$ contains no word of weight 4.

  Suppose $\mathcal{C}_{24}$ contained a set D of size 4. By Lemma 3.2.2(2), M is transitive on the 3-subsets of P, so we may assume that D has the form $\{0, 1, a, \infty\}$ with $a \in \mathbb{F}_{23}$. Let $E = \{0, 1, \infty\} \subset D$. There are $(24 \times 23 \times 22)/(3 \times 2 \times 1)$ 3-subsets of P, and the group M has order $24 \times 23 \times 11$ by Lemma 3.2.2(3). Thus, by the Orbit-Stabilizer Theorem, the setwise stabilizer of E has order 3. This stabilizer must be cyclic of order 3, generated by an element g. If g is expressed as the product of disjoint cycles, each cycle must be a 3-cycle or a fixed point, and so the number of fixed points must be divisible by 3.

  Suppose g has 3 or more fixed points. Then because M is transitive on 3-subsets of P, there is a non-trivial element $h \in M$ which fixes 0, 1 and ∞. Then h is an element of $M_{(\infty 0)} = S$ which fixes 1, and the only such element is the identity.

  Thus g has no fixed points, and in particular, g does not fix a. Then $D \triangle Dg = \{a, ag\}$ is an element of $\mathcal{C}_{24}$ of size 2, which we have already shown is impossible.

- $\mathcal{C}_{24}$ contains no word of weight 6.

  Suppose $\mathcal{C}_{24}$ contained a set D of size 6. Let E and F be two 3-element subsets of D. Because M is transitive on 3-subsets of P, there is a $g \in M$ such that $Eg = F$. Thus $Dg \cap D \supseteq F$ and must be of even size. It cannot have size 2, as $|F| > 2$. It cannot have size 4, or $Dg \triangle D \in \mathcal{C}_{24}$ would have size $(6-4)+(6-4) = 4$, which is impossible (no element of $\mathcal{C}_{24}$ has weight 4). So $Dg \cap D$ must have size 6, so $Dg = D$. So the setwise stabilizer M_D of D contains g. But there exists such a g for any 3-subsets E, F of D, so the setwise stabilizer of D acts transitively on the 3-subsets of D. There are $(6 \times 5 \times 4)/(3 \times 2 \times 1) = 20$ such 3-subsets, and by the Orbit-Stabilizer theorem, $20 \mid |M_D|$. But $M_D \leq M$ and $|M| = 24 \times 23 \times 11$, which is not divisible by 20, contradicting Lagrange's Theorem.

So the minimum distance is 8. ■

3.3 An outline of the MOG

There are many other constructions of the Golay code. One of the most useful for computation is the MOG (Miracle Octad Generator) of R. T. Curtis. The MOG is described in detail in chapter 11 of [CS99] and in [Gri98]. Here we give a brief outline, without going into detailed calculations or proofs.

Let $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ be the field of 4 elements with addition and multiplication tables given by Table 2. We define a code of length 6 over $\mathbb{F}_4$, called the *hexacode* $\mathcal{H}$, by:

$$\mathcal{H} = \{(a, b, c, a+b+c, a\bar{\omega}+b\omega+c, a\omega+b\bar{\omega}+c) : a, b, c \in \mathbb{F}_4\} \qquad (22)$$

It is clear that $\mathcal{H}$ is a 3-dimensional linear code. Codewords in $\mathcal{H}$ are called hexacodewords.

$+$	0	1	ω	$\bar{\omega}$
0	0	1	ω	$\bar{\omega}$
1	1	0	$\bar{\omega}$	ω
ω	ω	$\bar{\omega}$	0	1
$\bar{\omega}$	$\bar{\omega}$	ω	1	0

$\times$	1	ω	$\bar{\omega}$
1	1	ω	$\bar{\omega}$
ω	ω	$\bar{\omega}$	1
$\bar{\omega}$	$\bar{\omega}$	1	ω

Table 2: Addition and multiplication in $\mathbb{F}_4$

It is straightforward to check whether a given 6-tuple is a hexacodeword. Firstly, the 6-tuple must obey the *shape rule.* Split the 6 co-ordinates into 3 couples. Up to permuting the 3 couples or swapping the two elements of a couple, the 6-tuple must be of one of the following forms:

$$00\,00\,00, \qquad ab\,ab\,ab, \qquad 0a\,0a\,bc, \qquad aa\,bb\,cc, \qquad 00\,aa\,aa$$

where a, b and c are distinct non-zero elements of $\mathbb{F}_4$. Secondly, the 6-tuple must obey the *sign rule.* Associate each of the 3 couples with one of the numbers $\{-1, 0, +1\}$ as follows:

- $+1$ couples: 01, 0ω, $0\bar{\omega}$, 1ω, $\omega\bar{\omega}$, $\bar{\omega}1$
- -1 couples: 10, $\omega 0$, $\bar{\omega}0$, $\omega 1$, $\bar{\omega}\omega$, $1\bar{\omega}$
- 0 couples: 00, 11, $\omega\omega$, $\bar{\omega}\bar{\omega}$

A 6-tuple obeys the sign rule if either all the signs are 0, or the product of the signs is $+1$. A 6-tuple is a hexacodeword if it obeys the shape and sign rules. For example, it is easily seen that the 6-tuple $0\omega\,1\bar{\omega}\,\omega 0$ obeys both the shape and sign rules, so it is a hexacodeword.

A *MOG array* is a 4×6 binary matrix. Any column of a MOG array is associated with an element of $\mathbb{F}_4$ via the map

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \mapsto b + \omega c + \bar{\omega} d, \qquad a, b, c, d \in \mathbb{F}_2$$

This element of $\mathbb{F}_4$ is the *score* of the column. The *count* of any row or column of a MOG array is the number of non-zero digits it contains.

Definition 3.3.1 *A* MOG codeword *is a MOG array such that the scores of the array form a hexacodeword, and such that the count of each column and the top row are either all even or all odd.*

Conway in [CS99] verifies that that the MOG codewords form a $[24, 12, 8]$ code. One of the virtues of the MOG is that it is easy to check whether a given array is a codeword.

For example, the array:

1	0	1	1	0	0
0	0	0	1	0	1
0	1	1	1	1	1
0	0	1	0	0	1

has score 6-tuple $0\omega\,1\bar{\omega}\,\omega 0$, which is a hexacodeword (as we saw above) and the counts on the columns and the top row are all odd. Thus this MOG array is a codeword. On the other hand, the array:

1	0	1	0	1	1
1	1	1	0	0	0
1	0	0	0	0	1
1	1	0	0	1	0

has score 6-tuple $0\omega\,10\,\bar{\omega}\omega$, which is not a hexacodeword, so even though the counts on the columns and the top row have matching parities, this MOG array is not a codeword.

In section 4.1, we will see that the octads of a Golay code give an $S(5,8,24)$ Steiner system, and indeed, it is fairly easy to find the unique MOG octad containing a given 5-set by taking advantage of the error-correcting properties of the hexacode. The details are in chapter 11 of [CS99].

4 The relation $\mathcal{W}_{24} \sim \mathcal{C}_{24}$

There is a strong connection between the $S(5,8,24)$ Steiner system $\mathcal{W}_{24}$ and the extended binary Golay code $\mathcal{C}_{24}$. In this section, we will exhibit connections in both directions, in preparation for our definition of the large Mathieu groups in section 5. Along the way, we will see some nice properties of both structures.

4.1 The $S(5,8,24)$ Steiner system from a Golay code

Let $\mathcal{C}_{24}$ be any $[24,12,8]$ binary code on the set Ω (i.e. $\mathcal{C}_{24} \subseteq \mathcal{P}(\Omega)$ and $|\Omega| = 24$). An *octad* is a codeword of $\mathcal{C}_{24}$ with weight 8. In this section, we will show that the octads of $\mathcal{C}_{24}$ form an $S(5,8,24)$ Steiner system.

Let $\mathcal{C}_{24}^*$ be the set of cosets of $\mathcal{C}_{24}$ in $\mathcal{P}(\Omega)$, and let $\mathcal{C}_{24}^*(k)$ be the set of all cosets of $\mathcal{C}_{24}$ which contain a k-subset of Ω.

Lemma 4.1.1 *$\mathcal{C}_{24}^*$ is the disjoint union of the $\mathcal{C}_{24}^*(i)$ for $0 \le i \le 4$, and moreover:*

$$|\mathcal{C}_{24}^*(i)| = \begin{cases} \dbinom{24}{i} & \text{if } i = 0,\ 1,\ 2 \text{ or } 3 \\ \dbinom{24}{4}\Big/6 & \text{if } i = 4 \end{cases} \tag{23}$$

Proof We make the following elementary observation: If A and B are distinct subsets of Ω contained in the same coset of $\mathcal{C}_{24}$, then $A+B$ has weight at least 8 (as it is contained in $\mathcal{C}_{24}$, but is non-zero). The remark has these consequences:

1. If $0 \le i \le 3$, and C is a coset in $\mathcal{C}_{24}^*(i)$, then C contains a single i-subset of Ω, and no j-subsets (for $0 \le j \le 4, j \ne i$). Every such i-subset is contained in some coset of $\mathcal{C}_{24}^*(i)$, so the number $|\mathcal{C}_{24}^*(i)|$ of such cosets is exactly $\dbinom{24}{i}$.

2. If C is a coset in $\mathcal{C}_{24}^*(4)$, then C contains at most 6 other 4-subsets of Ω (because each the 4-subsets must be pairwise disjoint in order to get a codeword of weight 8), and no i-subsets for $i < 4$. Thus
$$|\mathcal{C}_{24}^*(4)| \geq \binom{24}{4} / 6 \tag{24}$$
3. The $\mathcal{C}_{24}^*(i)$ for $0 \leq i \leq 4$ are disjoint (if C were a coset in $\mathcal{C}_{24}^*(i)$ and $\mathcal{C}_{24}^*(j)$ for $0 \leq i < j \leq 4$, then C would contain both an i-subset and a j-subset, which we have already seen is impossible).

However, note that
$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \binom{24}{4} / 6 = 2^{12} = |\mathcal{C}_{24}^*| \tag{25}$$
so that the inequality (24) for $|\mathcal{C}_{24}^*(4)|$ must be an equality, and $\mathcal{C}_{24}^*$ must be the (disjoint) union of the $\mathcal{C}_{24}^*(i)$ for $0 \leq i \leq 4$. ■

Corollary 4.1.2 (Existence of sextets) *For any 4-subset E of Ω, there exists a partition of Ω into six 4-sets containing E such that the union of any two is an octad (such a partition is known as a* sextet*).*

Proof The 4-sets in a coset in $\mathcal{C}_{24}^*(4)$ must be pairwise disjoint, but no coset in $\mathcal{C}_{24}^*(4)$ can contain more than 6 pairwise disjoint 4-sets (because $24 = 4 \times 6$). Since there are only $\binom{24}{4}/6$ cosets in $\mathcal{C}_{24}^*(4)$, each must contain exactly 6 pairwise disjoint 4-sets.

Let $E_1 = E$ be any 4-subset of Ω, and let C be the coset containing E. Then $C \in \mathcal{C}_{24}^*(4)$, so C contains 5 other 4-sets $E_2, \ldots, E_6$ such that the E_i $(1 \leq i \leq 6)$ are pairwise disjoint. This gives us a partition of Ω into 4-sets. Since they are disjoint, the union of any two is equal to the sum of any two, and since each of the 4-sets is in C (a coset of $\mathcal{C}_{24}$), the sum of any two must be an 8-set in $\mathcal{C}_{24}$, that is, an octad. ■

Theorem 4.1.3 *The octads of $\mathcal{C}_{24}$ form an $S(5,8,24)$ Steiner system.*

Proof Let F be a 5-subset of Ω. We need to show that F is contained in a unique codeword of weight 8 in $\mathcal{C}_{24}$.

Existence: choose a 4-subset E_1 of F, and form the sextet $\{E_1, \ldots, E_6\}$. One of these 4-subsets (say E_2) must contain the point $F - E_1$. Then by Corollary 4.1.2, $E_1 + E_2$ is an octad containing F.

Uniqueness: suppose F were contained in distinct octads $A, B \in \mathcal{C}_{24}$. Then $A + B$ would be a non-empty set of size at most 6, which is impossible. ■

4.2 The Golay code from an $S(5,8,24)$ Steiner system

In this section we will go in the other direction, and show that the span of the blocks of $S(5,8,24)$ is a $[24,12,8]$ binary code. This will allow us to deduce the uniqueness of the Golay code (that is, $\mathcal{C}_{24}$ is the only $[24,12,8]$ linear code up to isomorphism).

Weight	Number of codewords
0	1
8	759
12	2576
16	759
24	1

Table 3: Weight distribution of $\mathcal{G}$

Let $\mathcal{G}$ be the vector subspace of $\mathcal{P}(\Omega)$ spanned by the blocks in $\mathcal{W}_{24}$.

We will investigate the ***weight distribution*** of $\mathcal{G}$: that is, we will determine (for each k) the number of codewords of weight k.

For this section, we will call codewords of weight 8 in $\mathcal{G}$ *octads*, and codewords of weight 12 *duodecads.*

Lemma 4.2.1 *If $A, B \in \mathcal{G}$ then $|A \cap B|$ is even.*

Proof Consider the non-singular inner product

$$(A, B) \mapsto |A \cap B| \pmod 2$$

. By Table 1 on page 4, the intersection of two blocks of $\mathcal{W}_{24}$ must be even. Thus the inner product of any two octads is 0. Since the octads span $\mathcal{G}$, the inner product of any two elements of $\mathcal{G}$ must be 0. ■

Theorem 4.2.2 *$\mathcal{G}$ has dimension 12, and has weight distribution given in Table 3.*

Proof We will prove this in several stages. In this proof, we will call a duodecad *normal* if it can be expressed as the sum of two octads.

1. *Claim:* A normal duodecad can be expressed as the sum of two octads in at most 132 ways (respecting order)

   Let D be a normal duodecad, and let F be a 5-subset of D. Because $\mathcal{W}_{24}$ is an $S(5, 8, 24)$ Steiner system, F is contained in a unique octad O_1. Now $|O_1 \cap D|$ must be even, and it must be at least 5, because $F \subseteq O_1 \cap D$. So $|O_1 \cap D|$ is either 6 or 8. If $|O_1 \cap D| = 8$, then $|O_1 \subseteq D|$, and the complement for O_1 in D is not an octad. However, if $|O_1 \cap D| = 6$, then $O_2 = O_1 + D$ is the unique octad satisfying $O_1 + O_2 = D$.

   Let K be the number of octads contained in D. Then the number of 5-subsets which give rise to an ordered octad decomposition for D is given by:

   $$\binom{12}{5} - K\binom{8}{5}$$

   (At the moment, all we know about K is that it is non-negative, but we will later see that $K = 0$.) For a decomposition $D = O_1 + O_2$, we have that $|D \cap O_1| = 6$, so there are 6 ways of choosing a 5-subset F to give any particular ordered decomposition into octads. Thus, the number of ordered pairs (O_1, O_2) of octads such that $O_1 + O_2 = D$ is given by:

$$\left[\binom{12}{5} - K\binom{8}{5}\right] \Big/ 6 \leq \binom{12}{5} \Big/ 6 = 132 \tag{26}$$

2. *Claim:* There are 340032 ways of choosing octads O_1, O_2 such that O_1+O_2 is a duodecad

   For octads O_1 and O_2, $O_1 + O_2$ is a duodecad if and only if $|O_1 \cap O_2| = 2$. The number of octads which have an intersection of size 2 with a given fixed octad O_1 is $\binom{8}{2} N_{2,8}$, so the number of ordered pairs (O_1, O_2) such that $O_1 + O_2$ is a duodecad is given by

   $$N_{0,0}\binom{8}{2} N_{2,8} = 340032 \tag{27}$$

3. *Claim:* There are at least 2576 normal duodecads.

   Given a normal duodecad D, there are at most 132 ways of writing it as the sum of two octads. However, there are 340032 ways of writing the sum of two octads to give a duodecad. Thus the number of normal duodecads must be at least $340032/132 = 2576$.

4. *Claim:* $\mathcal{G}$ has dimension 12.

   $\mathcal{W}_{24}$ is a spanning set of $\mathcal{G}$, and any two elements of $\mathcal{W}_{24}$ have even intersection. Thus $\mathcal{G}$ is contained in $\mathcal{G}^{\perp}$, the dual with respect to the standard inner product, so $\dim \mathcal{G} \leq 12$.

   On the other hand, $\mathcal{G}$ contains at least 2576 duodecads, and $2^{11} = 2048 < 2576 < 2^{\dim \mathcal{G}}$, so $\dim \mathcal{G} > 11$.

   Thus $\dim \mathcal{G} = 12$.

5. *Claim:* $\Omega \in \mathcal{G}$

   Because $\mathcal{G}$ has dimension 12 and is contained in its own dual, it must be a totally singular subspace. Ω has inner product 0 with every even subset, so it must be a member of $\mathcal{G}$.

6. *Claim:* The weight distribution table above is correct.

   We have accounted for the following codewords:

   - the empty codeword with weight 0;
   - at least 759 vectors of weight 8 (the original octads of $\mathcal{W}_{24}$)
   - at least 2576 vectors of weight 12
   - at least 759 vectors of weight 16 ($\Omega - O$ for each octad O)
   - a single vector of weight 24 (Ω itself).

   This gives a total of $4096 = 2^{12}$ vectors accounted for, and we cannot have any more because $\dim \mathcal{G} = 12$. Thus the table must be correct and complete. ■

Corollary 4.2.3 *$\mathcal{G}$ is a $[24, 12, 8]$ binary linear code.*

Proof This is immediate from the weight distribution table. ■

Corollary 4.2.4 *There is a unique* $[24, 12, 8]$ *binary code up to isomorphism, namely the Golay code* $\mathcal{C}_{24}$ *constructed in section 3.*

Proof We have shown that the octads of a Golay code form an $S(5,8,24)$ Steiner system, and that a Golay code is spanned by its octads. Since there is only one $S(5,8,24)$ Steiner system (up to isomorphism), this implies that there can only be one Golay code (up to isomorphism). ■

5 The large Mathieu groups

In the previous sections, we exhibited and showed the uniqueness of two combinatorical structures; namely, the $S(5,8,24)$ Steiner system $\mathcal{W}_{24}$ and the extended binary Golay code $\mathcal{C}_{24}$. We also saw how the blocks of a $S(5,8,24)$ Steiner system span a Golay code, and how the words of weight 8 in a Golay code form a Steiner system. Thus the automorphism groups of these two structures are isomorphic. Their common automorphism group is M_{24}, the largest Mathieu group.

5.1 Basic properties of M_{24}

Definition 5.1.1 *The* Mathieu group M_{24} *is the automorphism group of the unique binary extended Golay code (or equivalently, the unique* $S(5,8,24)$ *Steiner system).*

This group is one of the sporadic simple groups. It contains the other four Mathieu groups (and several other simple groups) as subgroups. We will now investigate some of its properties. The most striking property of M_{24} is given by the next theorem.

Theorem 5.1.2 M_{24} *is a 5-transitive group of degree 24.*

Proof Let $G = M_{24}$ acting on the $S(5,8,24)$ Steiner system $(\Omega, \mathcal{S})$. If we have any 3-set $Y = \{X_1, X_2, X_3\} \subseteq \Omega$, then $(\Omega, \mathcal{S})$ can be reconstructed from the projective plane $\Delta(Y)$ using the procedure in section 2.4. $PSL_3(4)$ is an automorphism of $(\Omega, \mathcal{S})$ fixing X_1, X_2 and X_3, because $PSL_3(4)$ preserves the hyperoval classes H_i and Fano subplane classes F_i used to construct $(\Omega, \mathcal{S})$. Thus $PSL_3(4)$ is a 2-transitive subgroup of the pointwise stabilizer $G_{(Y)}$. Hence G is 5-transitive. ■

Theorem 5.1.2 is important, because groups of high transitivity are rare. With the exception of the symmetric and alternating groups, there are only four finite groups whose degree of transitivity is greater than 3. This result follows from the Classification of Finite Simple Groups, because highly transitive groups are necessarily almost simple groups. We will meet the other three groups in this section and the next.

Corollary 5.1.3 M_{24} *is transitive on octads.*

Proof M_{24} is transitive on 5-sets, and each 5-set defines a unique octad. ■

Definition 5.1.4 *The* Mathieu group M_{24-i} *(for* $0 \leq i \leq 3$*) is the pointwise stabilizer of a set of* i *points in* M_{24} *(*M_{24} *is 5-transitive, so these groups are specified up to conjugacy).*

It is clear that M_{24-i} is $(5-i)$-transitive for $0 \leq i \leq 3$. The groups M_{24}, M_{23} and M_{22} (and sometimes M_{21}) are collectively known as the *large Mathieu groups.*

Theorem 5.1.5 $M_{21} \cong PSL_3(4)$

Proof Let $G = M_{24}$ acting on $(\Omega, \mathcal{S})$, $Y = \{X_1, X_2, X_3\}$, $M_{21} = G_{(Y)}$. We already know that $PSL_3(4) \lesssim G_{(Y)}$. The Steiner system $(\Omega, \mathcal{S})$ can be reconstructed from $\Delta(Y)$ in a different way for each re-ordering of the X_i, i.e. given any permutation $\sigma \in S_3$, we can find a $g \in G$ such that $X_i g = X_{i\sigma}$. Thus $G_Y/G_{(Y)}$ is the full symmetric group S_3, and so the pointwise stabilizer is an index 6 subgroup of the setwise stabilizer. But $PSL_3(4)$ is an index 6 subgroup of $P\Gamma L_3(4)$, and $P\Gamma L_3(4) \cong G_Y$, the setwise stabilizer. So, by comparing orders, we must have that $PSL_3(4) \cong G_{(Y)}$. ■

Theorem 5.1.6 *The orders of the large Mathieu groups are those given in Table 4*

Group	Degree	Order	
$M_{21} \cong PSL_3(4)$	21	20160	$= 21 \times 20 \times 48$
M_{22}	22	443520	$= 22 \times 21 \times 20 \times 48$
M_{23}	23	10200960	$= 23 \times 22 \times 21 \times 20 \times 48$
M_{24}	24	244823040	$= 24 \times 23 \times 22 \times 21 \times 20 \times 48$

Table 4: The large Mathieu groups

Proof The group M_{n-1} is the stabilizer of a point in M_n (we need Theorem 5.1.5), and:

$$|PSL_3(4)| = \frac{|SL_3(4)|}{3} = \frac{(4^3-1)(4^3-4)(4^3-4^2)}{3 \times 3}$$

The Orbit-Stabilizer Theorem gives us our result. ■

Lemma 5.1.7 *Let* O *be an octad.*

1. *The pointwise stabilizer of* O *in* M_{24} *is elementary abelian of order* 2^4*, acting regularly on* $\Omega - O$*.*

2. *The setwise stabilizer of* O *has an action of* A_8 *on* O*.*

3. *The setwise stabilizer of* O *is of the form* $2^4 A_8$*.*

Proof Let $G = M_{24}$, and let Y be a 3-subset of O. Then by Theorem 5.1.5, $G_{(O)}$ is the pointwise stabilizer in $PSL_3(4)$ of the line $O - Y$ in $\Delta(Y)$. Because $PSL_3(4)$ is 2-transitive, we may choose a particular line, say the set of points with first co-ordinate zero. But then, the pointwise stabilizer in $PSL_3(4)$ is isomorphic to the group of matrices of the form:

$$\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \qquad a, b \in \mathbb{F}_4 \tag{28}$$

which is elementary abelian of order 2^4. It is regular on $\Omega - O$, as there is precisely one group element which takes the point $(1, 0, 0)$ to $(1, a, b)$ for any $a, b \in \mathbb{F}_4$.

The setwise stabilizer G_O induces a 5-transitive action on O, and the pointwise stabilizer of Y in this action is isomorphic to $PSL_2(4)$ (because this is the setwise stabilizer in $PSL_3(4)$ of a line in the projective plane), which is isomorphic to A_5. Thus the action of G_O on O is isomorphic to A_8. Hence $G_O \cong 2^4 A_8$. ■

Lemma 5.1.8 *Let O be an octad, T a 2-subset of O, and H the pointwise stabilizer of O in M_{24}. Then H acts regularly on the set of octads which intersect O in T.*

Proof From Table 1 on page 4, we know there are 16 octads which intersect O in T.

Suppose that H does not act regularly on these 16 octads. Then because $|H| = 16$, there must be a non-trivial $h \in H$ and an octad O' such that h fixes O' setwise and $O' \cap O = T$. Now, h has order 2 and has no fixed points outside O (H acts regularly on $\Omega - O$ by Lemma 5.1.7), so it induces a permutation of cycle type 2^3 on O'. But h is in the setwise stabilizer of O', so the action of h should be an even permutation ($G_{O'}$ acts on O' like A_8). This is a contradiction. ■

Theorem 5.1.9 *M_{24} is transitive on duodecads.*

Proof By the above lemma, the pointwise stabilizer H of an octad acts transitively on the set of octads which intersect an octad O_1 in a particular 2-subset. By the proof of Theorem 4.2.2, any duodecad can be written as $O_1 + O_2$ (O_1, O_2 octads) with $|O_1 \cap O_2| = 2$. Since G acts transitively on octads (Corollary 5.1.3), we deduce that G acts transitively on duodecads. ■

5.2 Simplicity

To show that the large Mathieu groups are simple, we will need a result from the theory of permutation groups (proved in [DM96] and chapter 9 of [Rot84]).

Theorem 5.2.1 *Let G be a group acting faithfully and k-transitively ($k \geq 2$) on a set X with $|X| = n$. Suppose the stabiliser G_x of a single element is a simple group. Then one of the following possibilities holds:*

- *G is a simple group.*

- *$k = 2$ and n is a prime power.*
- *$k = 3$ and n is a power of 2.*
- *$k = 3$, n is not a power of 2, and $G \cong S_3$*

We will need a technical lemma for the proof of Theorem 5.2.1.

Lemma 5.2.2 *If G is transitive on X and $H \lhd G$ is regular, then for any $x \in X$, the induced action of G_x on $X - \{x\}$ and the conjugation action (indicated by $\star$) of G_x on $H - \{1\}$ are G_x-isomorphic.*

Proof Let $\theta : H - \{1\} \to X - \{x\}$ be the map $h \mapsto xh$. Note that $xh \neq x$, as $h \neq 1$ and H is regular. To show that θ is a G_x-morphism, we need to show that for any $g \in G_x$ and $h \in H - \{1\}$:

$$(h \star g)\theta = (h\theta)g \tag{29}$$

But $h \star g = g^{-1}hg$, so $(h \star g)\theta = x(g^{-1}hg) = xhg$, since g^{-1} stabilises x. On the other hand, $(h\theta)g = xhg$, so equation (29) holds, and θ is a G_x-morphism. The map θ is surjective (as H is transitive) and injective (if $xh_1 = xh_2$, then $h_1h_2^{-1} \in H_x$, and $H_x = 1$ as H is regular). Hence θ is a G_x-isomorphism. ■

Proof of Theorem 5.2.1. Suppose G is not simple, and let H be a non-trivial proper normal subgroup of G. Since G is at least 2-transitive, G is primitive. Thus H is a normal subgroup of a primitive group, and so is transitive.

Let x be an arbitrary element of X. Then $H \cap G_x \lhd G_x$, and G_x is simple (all one-point stabilisers in G are isomorphic, since G is transitive). Therefore, $H \cap G_x$ is either trivial or the whole of G_x. Suppose it is the whole of G_x. Then we have $G_x \subseteq H \subsetneq G$. But G is primitive, so G_x is a maximal subgroup of G, which implies $H = G_x$, contradicting the transitivity of H. Thus $H \cap G_x$ must be trivial for all $x \in X$, and H must be regular, giving $|H| = n$.

Now, the action of G_x on $X - \{x\}$ is $(k-1)$-transitive, so the action of G_x on $H - \{1\}$ by conjugation is $(k-1)$-transitive (Lemma 5.2.2 says that the actions are G_x-isomorphic). We note the following facts:

- Since $k \geq 2$, G_x acts transitively on $H - \{1\}$ by conjugation. Conjugation is an automorphism, so all elements of $H - \{1\}$ have the same order, which must be a prime p. So H is a p-group, and so $Z(H)$ is non-trivial. Since it is a characteristic subgroup, we must have $Z(H) = H$. Thus H is elementary abelian of order $n = p^s$ for some s.

- If $k \geq 3$, then G_x acts 2-transitively (and hence primitively) on $H - \{1\}$. But for any $h \in H - \{1\}$, $\{h, h^{-1}\}$ is a block, so it is either a singleton or the whole of H. If $h \neq h^{-1}$ for some $h \in H - \{1\}$, then $|H| = 3$, whence $H \cong \mathbb{Z}_3$. Otherwise $h = h^{-1}$ for all $h \in H - \{1\}$, whence H is an elementary abelian 2-group.

- If $k \geq 4$, then G_x acts 3-transitively on $H - \{1\}$, so in particular $|H| \geq 4$, so H must be a non-cyclic elementary abelian 2-group. H contains a subgroup $V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, with generators h and h' say. Now the stabiliser $(G_x)_h$ of h in G_x acts 2-transitively (and hence primitively) on $H - \{1, h\}$. But $\{h', hh'\}$ is a block for $(G_x)_h$, so $H - \{1, h\} = \{h', hh'\}$, and so $H = V$.

Thus if $k = 2$, then $H \cong \mathbb{Z}_p^n$ for some n, and hence $n = |H|$ is a prime power. If $k = 3$, then either $H \cong \mathbb{Z}_2^n$ for some n (so n is a power of 2) or $|H| = 3$, in which case $G \cong S_3$, as the only 3-transitive subgroup of S_3 is S_3 itself. If $k \geq 4$, then $n = 4$, and the only 4-transitive subgroup of S_4 is S_4, so $G \cong S_4$. But then $G_x \cong S_3$, which is not a simple group, which is a contradiction. Thus we have accounted for all the possibilities. ■

Corollary 5.2.3 *M_{22}, M_{23} and M_{24} are simple groups.*

Proof The stabilizer of one point in M_{22} is $PSL_3(4)$, which is a simple group (by a well-known theorem of Jordan and Dickson: see Theorem 8.27 in [Rot84]). M_{22} is 3-transitive on 22 points. 22 is not a power of 2, and M_{22} is clearly not S_3. Therefore, by Theorem 5.2.1, M_{22} is simple.

The stabilizer of one point in M_{23} is M_{22}, which is simple. M_{23} is 4-transitive, so by Theorem 5.2.1, M_{23} is simple.

The stabilizer of one point in M_{24} is M_{23}, so by the same argument, M_{24} is simple. ■

6 The little Mathieu groups

Let M_{24} act on the Golay code $\mathcal{C}_{24}$ (a set of subsets of Ω). We will investigate the little Mathieu groups M_{12} and M_{11} as certain stabilizers of sets in M_{24}.

6.1 Definitions and basic properties

Definition 6.1.1 *The* Mathieu group M_{12} *is the setwise stabilizer of a duodecad in M_{24}. (M_{24} is transitive on duodecads by Theorem 5.1.9, so the duodecad chosen does not matter.)*

Choose a duodecad D and let $D' = \Omega - D$. For the rest of this section, M_{12} acts on Ω, sending D to D.

We now define a set system $(\Omega_D, \mathcal{S}_D)$ by:

$$\Omega_D = D; \qquad \mathcal{S}_D = \{D \cap O : O \in \mathcal{S}, |D \cap O| = 6\} \tag{30}$$

Theorem 6.1.2 *$(\Omega_D, \mathcal{S}_D)$ is a $S(5,6,12)$ Steiner system.*

Proof Two octads of $(\Omega, \mathcal{S})$ never share a 5-element subset, so the same is true for the blocks of $\mathcal{S}_D$. On the other hand, the number of blocks in $\mathcal{S}_D$ is 132 (the number of ways D can be written as the sum of two octads, from the proof of Theorem 4.2.2), which is the same as $\binom{12}{5} \Big/ \binom{6}{5}$ (the number of 5-subsets of D). Thus any 5-subset of D is contained in a unique block in $\mathcal{S}_D$. ■

Theorem 6.1.3 *M_{12} acts transitively on the blocks of $\mathcal{S}_D$.*

Proof Let B_1, B_2 be blocks in $\mathcal{S}_D$ contained in octads O_1 and O_2 respectively. There exists octads O_1' and O_2' such that $D = O_1 + O_1'$ and $D = O_2 + O_2'$. Since M_{24} is transitive on octads, there exists $g \in M_{24}$ such that $O_1 g = O_2$. Note that $O_1' g$ and O_2' intersect O_2 in the same 2-subset (the 2-subset of O_2 which is outside the duodecad D), so by Lemma 5.1.8, there exists $h \in (M_{24})_{(O_2)}$ such that $(O_1' g)h = O_2'$. It is clear that $O_1 gh = O_2$, so $Dgh = D$. Thus $gh \in M_{12}$ and $B_1 gh = B_2$. ■

Theorem 6.1.4 *M_{12} acts faithfully and 5-transitively on the points of D. Its order is $|M_{12}| = 12 \times 11 \times 10 \times 9 \times 8 = 95040$, so M_{12} is sharply 5-transitive.*

Proof Let $G = M_{24}$. Let B_1 be a block in $\mathcal{S}_D$, contained in the unique octad O_1, and let $O_2 = D - O_1$, $B_2 = D \cap O_2$. Then B_2 is a block in $\mathcal{S}_D$ and D is the disjoint union of B_1 and B_2. Let $T = O_1 \cap O_2$; this is a 2-subset of $\Omega - D$.

Let H be the subgroup of G stabilizing both B_1 and B_2. Since $G_{(O_1)}$ acts regularly on the octads which intersect O_1 in T, and G_{O_1} has the action of A_8 on the points of O_1, we find that H is the setwise stabilizer of T in G_{O_1}; and this is S_6. So H induces faithful 6-transitive actions on B_1 and B_2. Now H is the setwise stabilizer of B_1 in M_{12}, so the fact that M_{12} is transitive on blocks of $\mathcal{S}_D$ gives the faithful 5-transitive action on the points of D. The order of the group follows directly from the Orbit-Stabilizer Theorem. ■

So M_{12} is our second "non-trivial" 5-transitive group. As we remarked earlier, there are no others (apart from alternating and symmetric groups).

An interesting corollary is that an outer automorphism of S_6 is visible inside M_{12}. Let F_1 be any 4-subset of B_1, and let $\mathbb{S} = \{F_1, F_2, \ldots, F_6\}$ be the sextet containing F_1. The symmetric difference of two words of $\mathcal{C}_{24}$ is a word in $\mathcal{C}_{24}$, so the intersection of an octad and a duodecad can only have size 2, 4 or 6. Thus for each $2 \leq i \leq 6$, $|(F_1 \cup F_i) \cap D| \in \{2, 4, 6\}$, and hence $|F_i \cap D| \in \{0, 2\}$.

Hence a 4-subset of B_1 corresponds to a partition of B_2 into three 2-subsets, so the S_6-actions of H on the two blocks must be inequivalent. (For example, a 3-cycle of points in F_1 cannot change the partition of B_2, so it must map to a permutation of shape 3^2.) An element $g \in M_{12}$ that swaps the two blocks induces an outer automorphism of S_6, and such a g exists because M_{12} is transitive on blocks by Theorem 6.1.3. ■

Definition 6.1.5 *The* Mathieu group M_{11} *is the stabilizer of any point $P \in D$ in M_{12} (up to conjugacy, it does not matter which point is chosen, as M_{12} is 5-transitive).*

Corollary 6.1.6 *M_{11} acts faithfully on the points of $D - \{P\}$, and the action is sharply 4-transitive. The order of the group is $|M_{11}| = 11 \times 10 \times 9 \times 8 = 7920$.*

6.2 The 3-transitive action of M_{11}

Note that M_{12} is also the setwise stabilizer of D', and thus has a faithful 5-transitive action on the 12 points of D'. However, the actions of M_{12} on D and D' are not equivalent, because the stabilizer in M_{12} of a block $B \subseteq D$ acts 6-transitively on the points of B and the points of $D - B$, whereas this same stabilizer fixes a 2-subset of D'. In the same way that we found an outer automorphism of S_6 by swapping blocks of $\mathcal{S}_D$, we can get an outer automorphism of

M_{12} by swapping a duodecad with its complement (which is certainly possible, as M_{24} is transitive on duodecads).

Let P be an arbitrary point of D. The stabilizer of P in M_{12} is the group M_{11}. Consider the action of this group in the complementary duodecad D' (think of M_{11} as a subgroup of $Sym(D')$). This group cannot fix any point, or else the actions of M_{12} on the two duodecads would be equivalent. Since 11 divides the order of M_{11}, there must be an element of order 11, i.e. an 11-cycle. Since M_{11} is not a point stabilizer, M_{11} is 2-transitive. Let K be the stabilizer of two points of D'. Then $|K| = 7920/(12 \times 11) = 60$, so K must contain an element of order 5. Thus on the remaining 10 points, either K is transitive, or it has two orbits of size 5. Suppose the latter. Then K contains an element x of order 3 whose cycle decomposition can has at most one 3-cycle on each orbit, which means x fixes at least 6 points of D'. But this is impossible, since M_{12} is sharply 5-transitive. So K is transitive on the remaining 10 points, and thus:

Theorem 6.2.1 *M_{11} has a 3-transitive action on 12 points.* ■

6.3 Simplicity

The main result in this section is from [Cha95].

Lemma 6.3.1 *Let p be a prime, and let G be a transitive subgroup of S_p. Let m_G be the number of Sylow p-subgroups, and let r_G be the index of a Sylow p-subgroup in its normalizer.*

1. *G has cyclic Sylow p-subgroups.*
2. *$|G| = pr_Gm_G$.*
3. *r_G is the least positive residue of $|G|/m_G$.*
4. *If $m_G > 1$, then $r_G > 1$.*

Proof Since G is transitive, $p \mid |G|$, but p^2 does not divide $p!$, so the Sylow p-subgroups of G must be cyclic of order p. This proves (1). Let P be a Sylow p-subgroup; without loss of generality, we may assume that $P = \langle (12 \dots p) \rangle$.

The normalizer $N_G(P)$ of P consists of permutations of the form:

$$\mathbb{Z}_p \to \mathbb{Z}_p, \qquad x \mapsto ax + b \qquad (a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p)$$

There are $p(p-1)$ such transformations in S_p, so $|N_G(P)| \mid p(p-1)$, and hence $r_G = |N_G(P)|/|P|$ is a factor of $p-1$.

By Sylow's Theorem, all the Sylow p-subgroups are conjugate, so:

$$|G| = |P||N_G(P) : P||G : N_G(P)| = pr_Gm_G \tag{31}$$

which proves (2). Moreover $m_G \equiv 1 \pmod p$ and since $r_G \mid p-1$ (and in particular, $0 < r_G < p$) we see that r_G is the least residue (mod p) of $|G|/p$, thus proving (3).

Finally, suppose $m_G > 1$ and $r_G = 1$. The group G is transitive, so by the Orbit-Stabilizer Theorem, each point stabilizer G_i has size $|G|/p = m_Gr_G = m_G$. However, the number of elements of order p is $m_G(p-1) = n - m_G$, so G

has at most m_G elements that fix any element at all. So all the point-stabilizers must be equal. But then if $g \in G$ fixes any element, it fixes them all, so $g = 1$. So all the point-stabilizers are trivial, and $m_G = 1$, which is a contradiction. This proves (4). ■

Theorem 6.3.2 *M_{11} is simple.*

Proof We will use the notation of Lemma 6.3.1. Let $G = M_{11}$, $p = 11$: we have observed that G is a transitive subgroup of S_{11}, with order 7920. Note that $7920/11 = 720 \equiv 5(\pmod{11})$, so by 6.3.1 we must have $r_G = 5$, $m_G = 144$.

Let H be a non-trivial normal subgroup of G: we want to show that $H = G$. Since G is 4-transitive, G is primitive, so the normal subgroup H is transitive. Hence $P \leq H$ for some Sylow 11-subgroup P of G. By Sylow's Theorems, all the Sylow 11-subgroups of G are conjugate to P, so by normality, H contains all the Sylow 11-subgroups of G. Thus $m_H = m_G = 144$, so by Lemma 6.3.1, $|H| = pm_Hr_H = 11 \times 144 \times r_H$. By Lagrange's Theorem, $|H| \mid |G|$, so $r_H \mid r_G = 5$. But $r_H \neq 1$ by 6.3.1, so $r_H = 5$. Hence $|H| = |G|$, and $H = G$. ■

A very similar argument could be used to prove that M_{23} is simple.

Corollary 6.3.3 *M_{12} is simple.*

Proof M_{11} is the one-point stabilizer of M_{12}, and it is a simple group. By Theorem 5.2.1, a 5-transitive group with a simple one-point stabilizer is simple, and we have shown that M_{12} is 5-transitive on 12 points. Hence M_{12} is simple. ■

7 The Leech lattice Λ

A *lattice of dimension n* is a free abelian subgroup of $\mathbb{R}^n$ with n generators. In this final section, we will construct a particular 24-dimensional lattice Λ (the *Leech lattice*) and examine Co_0, its group of automorphisms. We will see some connections with the Mathieu groups.

7.1 Construction and basic properties of Λ

We will follow the construction of Λ given in [Con99].

Let Ω be the projective line on $\mathbb{F}_{23}$, with elements $0, 1, \ldots, 22, \infty$ as usual. Let $\mathcal{C}_{24}$ be the extended binary Golay code on Ω, as constructed in section 3.2. Label an orthonormal basis of $\mathbb{R}^{24}$ by e_i, $i \in \Omega$, and for any subset $S \subseteq \Omega$, let $v_S = \sum_{i \in S} e_i$.

Definition 7.1.1 *The Leech lattice Λ is the vector subspace of $\mathbb{R}^{24}$ spanned by the vectors of $2v_O$ (where O is an octad in $\mathcal{C}_{24}$), together with the vector $v_\Omega - 4e_\infty$.*

Note that an n-dimensional lattice has an inner product inherited from the Euclidean inner product of $\mathbb{R}^n$.

Lemma 7.1.2 *For any two vectors $x, y \in \Lambda$, the inner product $x.y$ is divisible by 8, and the inner product $x.x$ is divisible by 16.*

Proof For any two of our generating vectors x, y, we can verify that $x.y$ is divisible by 8 (recall that two octads intersect in 0, 2, 4 or 8 places). By linearity, this applies to any $x, y \in \Lambda$. Now:

$$(x+y).(x+y) = (x.x) + (y.y) + 2(x.y) \tag{32}$$

and since $x.x$ is divisible by 16 for any generating vector x, and $x.y$ is divisible by 8 for any $x, y \in \Lambda$, we must have that $x.x$ is divisible by 16 for any $x \in \Lambda$. ■

Lemma 7.1.3 *We have:*

1. *For any 4-set F, $4v_F \in \Lambda$.*
2. *For any two elements $i, j \in \Omega$, $4e_i - 4e_j \in \Lambda$.*

Proof

1. We know from Corollary 4.1.2 that we can find a sextet containing F. If F_1 and F_2 are two of the other 4-sets in the sextet, then $F \cup F_1$, $F \cup F_2$ and $F_1 \cup F_2$ are octads. Thus:

$$4v_F = 2v_{F\cup F_1} + 2v_{F\cup F_2} - 2v_{F_1\cup F_2} \tag{33}$$

   and so $4v_F \in \Lambda$.

2. Pick 3 elements k_1, k_2, k_3 distinct from i and j. Then let $F_1 = \{i, k_1, k_2, k_3\}$ and $F_2 = \{j, k_1, k_2, k_3\}$. From the first part, we know that $4v_{F_1}$ and $4v_{F_2}$ are in Λ, and thus $4e_i - 4e_j = 4v_{F_1} - 4v_{F_2} \in \Lambda$. ■

Theorem 7.1.4 *A vector $x = (x_0, x_1, \ldots, x_{22}, x_\infty)$ with integral co-ordinates is in Λ if and only if the following three conditions hold:*

1. *There exists an m such that for all $i \in \Omega$, $x_i \equiv m \pmod 2$.*
2. *For each k, the set $\{i \in \Omega : x_i \equiv k \pmod 4\}$ is a codeword in $\mathcal{C}_{24}$.*
3. *We have $\sum_{i\in\Omega} x_i \equiv 4m \pmod 8$*

Proof All three statements are true for the generators of Λ, so hold for all vectors $x \in \Lambda$ by linearity.

Conversely, suppose $x \in \mathbb{R}^{24}$ satisfies all three conditions. To show $x \in \Lambda$, we will add vectors from Λ to x until we get a vector which is obviously an element of Λ.

Let $y = x + c(v_\Omega - 4v_\infty)$, where c is an integer chosen so that all the co-ordinates of y are even, and their sum is a multiple of 16.

Let A be the set of co-ordinates of y congruent to 2 (mod 4). Then A is a codeword in $\mathcal{C}_{24}$, and since $\mathcal{C}_{24}$ is spanned by its octads, we may write $A = O_1 \triangle \ldots \triangle O_n$ for octads $O_1, \ldots, O_n$. Then if $z = y - 2v_{O_1} - \ldots - 2v_{O_n}$, then all the co-ordinates of z are divisible by 4, and the sum of the co-ordinates is a multiple of 16.

But the space of such vectors is spanned by $4v_F$ (for F a 4-set) and $4e_i - 4e_j$ (for $i \neq j$), and these vectors are in Λ by Lemma 7.1.3. Thus our original vector x must be in Λ. ■

Corollary 7.1.5 *Λ is a 24-dimensional lattice.*

Proof From Theorem 7.1.4, we know that $8v_i \in \Lambda$ for each $i \in \Omega$ (24 elements), and these vectors are clearly linearly independent over $\mathbb{R}$. ■

7.2 Types and shapes of vectors in Λ

In this section, we give a partial classification of the small vectors in Λ.

Let $\Lambda(n)$ be the set of all vectors $x \in \Lambda$ satisfying $x.x = 16n$. In this case, we say x is of *type* n. Moreover, we say that x is of *type* n_{ab} if it is of type n and can be written as the sum of a vector of type a and a vector of type b.

The *shape* of a vector $x \in \Lambda$ is an expression of the form $(a_1^{n_1} \cdot a_2^{n_2} \cdot \ldots \cdot a_r^{n_r})$, where n_i is the number of co-ordinates of x taking the value $|a_i|$ (our definition of the shape of a vector disregards the sign).

By a number of straightforward arguments using Theorem 7.1.4 and the weight distribution table (Table 3 on page 25), we can count the number of vectors of each shape. For example, to count the vectors of shape $(2^{12}0^{12})$, observe that the co-ordinates taking the values ± 2 must be a word of weight 12 in $\mathcal{C}_{24}$ (2576 such), and there are 2^{12} ways of choosing the signs for the first 11 co-ordinates, and the last sign is determined by the fact that the sum of co-ordinates is congruent to 0 (mod 8). Thus there are $2^{11} \times 2576$ vectors of this shape. All shapes of type ≤ 4 are enumerated in Table 5 below (based on Table 4.13 from [CS99]).

Type	Shape	Number of vectors	
0	(0^{24})		1
1	none		0
2	$(3^1 \cdot 1^{23})$	$2^{12} \cdot 24$	98304
	$(2^8 \cdot 0^{16})$	$2^7 \cdot 759$	97152
	$(4^2 \cdot 0^{22})$	$2^2 \cdot \binom{24}{2}$	1104
3	$(2^{12} \cdot 0^{12})$	$2^{11} \cdot 2576$	5275648
	$(3^3 \cdot 1^{21})$	$2^{12} \cdot \binom{24}{3}$	8290304
	$(4 \cdot 2^8 \cdot 0^{15})$	$2^8 \cdot 759 \cdot 16$	3108864
	$(5 \cdot 1^{23})$	$2^{12} \cdot 24$	98304
4	$(2^{16} \cdot 0^8)$	$2^{11} \cdot 759 \cdot 16$	24870912
	$(3^5 \cdot 1^{19})$	$2^{12} \cdot \binom{24}{5}$	174096384
	$(4^4 \cdot 0^{20})$	$2^4 \cdot \binom{24}{4}$	170016
	$(4^2 \cdot 2^8 \cdot 0^{14})$	$2^9 \cdot 759 \cdot \binom{16}{2}$	46632960
	$(4 \cdot 2^{12} \cdot 0^{11})$	$2^{12} \cdot 2576 \cdot 12$	126615552
	$(5 \cdot 3^2 \cdot 1^{21})$	$2^{12} \cdot \binom{24}{3} \cdot 3$	24870912
	$(6 \cdot 2^7 \cdot 0^{16})$	$2^7 \cdot 759 \cdot 8$	777216
	$(8 \cdot 0^{23})$	$2^1 \cdot 24$	48

Table 5: Shapes and types of small vectors in the Leech lattice

Note that Theorem 7.1.4 implies that $\Lambda(1)$ is empty. We say that Λ has no *roots*. Thus the *kissing number* (number of equally-sized non-overlapping spheres that all touch another sphere of the same size) for this lattice is given by $|\Lambda(2)| = 196560$; this is in fact the optimal kissing number for 24 dimensions. A proof of this remarkable fact is given in chapter 13 of [CS99].

7.3 The automorphism group Co_0

Definition 7.3.1 *The* Conway group Co_0 *is the group of Euclidean congruences of* $\mathbb{R}^{24}$ *that fix the origin and preserve* Λ. *(That is,* Co_0 *is the automorphism group of* Λ.*)*

If we fix a basis or $\mathbb{R}^{24}$, the elements of Co_0 can be thought of as real orthogonal (24×24) matrices. Since $8e_i \in \Lambda$, we see that the entries of the matrix must be rational with denominator dividing 8.

For any permutation π of Ω, we can think of π as a Euclidean congruence, with the action given by $e_i\pi = e_{i\pi}$. For any subset $S \subseteq \Omega$, define the congruence ϵ_S by:

$$e_i\epsilon_S = \begin{cases} e_i & \text{if } i \notin S \\ -e_i & \text{if } i \in S \end{cases} \tag{34}$$

Let N be the set of congruences of the form $\pi\epsilon_C$ for $C \in \mathcal{C}_{24}$, $\pi \in Sym(\Omega)$.

A technical lemma:

Lemma 7.3.2 $\lambda \in N$ *if and only if* $\lambda \in Co_0$ *and* $e_i\lambda = \pm e_j$ *for some* $i, j \in \Omega$.

Proof The forward implication is obvious. To prove the converse, consider the matrix of λ. Its ith row must contain ± 1 in the jth column and 0s elsewhere. Since λ is orthogonal, the jth place of all the other rows must be 0:

$$\begin{bmatrix} * & \dots & \dots & 0 & \dots & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ * & \dots & \dots & 0 & \dots & \dots & * \\ 0 & \dots & 0 & \pm 1 & 0 & \dots & 0 \\ * & \dots & \dots & 0 & \dots & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ * & \dots & \dots & 0 & \dots & \dots & * \end{bmatrix}$$

For any $k \in \Omega$, the vector $4e_i + 4e_k \in \Lambda$ is of type 2, so its image under λ must be of type 2, and since it is 4 times the sum of rows i and k in λ, it must have a co-ordinate ± 4. Table 5 then tells us that that $(4e_i + 4e_k)\lambda$ has shape $(4^2 0^{22})$, so the kth row of λ contains a single co-ordinate ± 1 and the rest 0 (and again, by orthogonality, all the other rows must have a 0 in this column).

Thus $\lambda = \pi\epsilon_C$ for some permutation π and some $C \subseteq \Omega$. We need to show $C \in \mathcal{C}_{24}$. Consider the vector $(v_\Omega - 4e_\infty)\lambda$. This is a vector of Λ, so the co-ordinates congruent to 3 (mod 4) must be a codeword in $\mathcal{C}_{24}$. But these co-ordinates are precisely the co-ordinates labelled by C. So $C \in \mathcal{C}_{24}$. ■

Corollary 7.3.3 N *is a subgroup of* Co_0 *of the form* $2^{12}M_{24}$ *(split extension).*

Proof N is certainly a subset of Co_0. To show that it is a subgroup, let $\lambda_1, \lambda_2 \in N$ and set $\lambda = \lambda_1 \lambda_2^{-1}$. To show $\lambda \in N$, note that $\lambda \in Co_0$ and $e_1\lambda = \pm e_i$ for some i. So by Lemma 7.3.2, $\lambda \in N$.

Now $\lambda = \pi\epsilon_C$ for some permutation π and some set $C \in \mathcal{C}_{24}$. For an arbitrary codeword S, $(2v_S)\lambda$ has non-zero co-ordinates in the places of $S\pi$, so π preserves $\mathcal{C}_{24}$. Hence $\pi \in M_{24}$, and since the subgroup $\{\epsilon_C : C \in \mathcal{C}_{24}\}$ (isomorphic to 2^{12}) in N is a normal subgroup of N, we have $N = 2^{12}M_{24}$. ■

Thus we see immediately that Co_0 has all the Mathieu groups as subgroups. There are other interesting subgroups.

We cannot hope for Co_0 to be transitive on Λ, because it preserves the lengths of vectors. However, it is not unreasonable to hope that it is transitive on $\Lambda(n)$ for particular values of n. This is certainly not the case for N, because N preserves vector shape. Thus we suspect that N is a proper subgroup of Co_0.

Let F be any 4-set. Then there is a sextet $\mathbb{S} = \{F_1, \dots, F_6\}$ with $F = F_1$. Consider the map η given by:

$$e_i\eta = e_i - \frac{1}{2}v_{F_j} \qquad \text{for } i \in F_j \tag{35}$$

and let $\xi = \eta\epsilon_F$. It is clear that $\xi \notin N$, since ξ maps vectors of shape $(8 \cdot 0^{23}))$ to vectors of shape $(4^4 \cdot 0^{20})$. However:

Lemma 7.3.4 $\xi \in Co_0$

Proof This is a straightforward, if messy, calculation. We will show that ξ sends each generator of Λ to another element of Λ.

We will represent vectors by strings of 24 symbols, split into tetrads, and where $\overline{n}$ is a shorthand for $-n$. Throughout the proof, we will relabel co-ordinates as necessary.

For the generator $x = v_\Omega - 4v_\infty$, we have:

$$\begin{aligned} x =& \overline{3}111 \quad 1111 \quad 1111 \quad 1111 \quad 1111 \quad 1111 \\ x\eta =& \overline{3}111 \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \\ x\xi =& \begin{cases} 3\overline{111} \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \\ \overline{3}111 \quad 1111 \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \quad \overline{1111} \end{cases} \end{aligned}$$

where the two possibilities are representative for the different choices for F.

The other generators are of the form $x = 2v_O$ for an octad O. One of the following possibilities holds:

1. O is the union of 2 tetrads of $\mathbb{S}$.

$$\begin{aligned} x =& 2222 \quad 2222 \quad 0000 \quad 0000 \quad 0000 \quad 0000 \\ x\eta =& \overline{2222} \quad \overline{2222} \quad 0000 \quad 0000 \quad 0000 \quad 0000 \\ x\xi =& \begin{cases} \overline{2222} \quad \overline{2222} \quad 0000 \quad 0000 \quad 0000 \quad 0000 \\ \overline{2222} \quad 2222 \quad 0000 \quad 0000 \quad 0000 \quad 0000 \end{cases} \end{aligned}$$

2. O contains 2 points from each of 4 tetrads of $\mathbb{S}$.

$$\begin{aligned} x =& 2200 \quad 2200 \quad 2200 \quad 2200 \quad 0000 \quad 0000 \\ x\eta =& 00\overline{22} \quad 00\overline{22} \quad 00\overline{22} \quad 00\overline{22} \quad 0000 \quad 0000 \\ x\xi =& \begin{cases} 00\overline{22} \quad 00\overline{22} \quad 00\overline{22} \quad 00\overline{22} \quad 0000 \quad 0000 \\ 0022 \quad 00\overline{22} \quad 00\overline{22} \quad 00\overline{22} \quad 0000 \quad 0000 \end{cases} \end{aligned}$$

3. O contains 3 points from 1 tetrad of $\mathbb{S}$ and 1 from each of the other 5.

$$\begin{aligned} x =& 2220 \quad 2000 \quad 2000 \quad 2000 \quad 2000 \quad 2000 \\ x\eta =& \overline{1113} \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \\ x\xi =& \begin{cases} 1113 \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \\ \overline{1113} \quad \overline{1}111 \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \quad 1\overline{111} \end{cases} \end{aligned}$$

In each of these cases, by Theorem 7.1.4, $x\xi \in \Lambda$. Hence $\xi \in Co_0$. ■

Lemma 7.3.5 *Co_0 is transitive on $\Lambda(2)$, $\Lambda(3)$ and $\Lambda(4)$*

Proof The orbits of N in $\Lambda(2)$, $\Lambda(3)$ and $\Lambda(4)$ are determined exactly by the vector shape, *except* for the shape $(2^{16} \cdot 0^8)$, where there are two orbits (see Table 6).

Orbit	Typical vector	Size of orbit
$(2^{16} \cdot 0^8)^+$:	0000 0000 2222 2222 2222 2222	$2^{11} \cdot 759$
$(2^{16} \cdot 0^8)^-$:	0000 0000 $\overline{22}22$ 2222 2222 2222	$2^{11} \cdot 759 \cdot 15$

Table 6: Vectors of shape $(2^{16} \cdot 0^8)$ under N

The orbits of N on $\Lambda(n)$ (for $n = 2, 3, 4$) fuse under the action of the whole group. To show this, we choose a suitable vector x from each N-orbit, and see that $x\xi$ is in a different N-orbit. The details are given in Table 7. Note that the vectors in the table are in fact in Λ (for a suitable labelling of the co-ordinates). As before, we show the six textrads of a sextet separately. ■

By Lemma 7.3.2, the set $\{\pm 8e_i : i \in \Omega\}$ is a block of imprimitivity for the action of Co_0 on $\Lambda(4)$. The other blocks (sets of 48 vectors in 24 mutually orthogonal pairs) are called *co-ordinate frames.*

Theorem 7.3.6 *Every vector $x \in \Lambda$ is congruent (mod 2Λ) to exactly one of the following:*

- *The vector 0*
- *Each vector of a unique pair x, $-x$, with $x \in \Lambda(2)$*
- *Each vector of a unique pair x, $-x$, with $x \in \Lambda(3)$*
- *Each of the 48 vectors of a co-ordinate frame in $\Lambda(4)$*

	N-orbits	x and $x\xi$					
$\Lambda(2)$	$(2^8 \cdot 0^{16})$	2220	2220	2000	2000	2000	2000
	$(3^1 \cdot 1^{23})$	1113	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$
	$(4^2 \cdot 0^{22})$	4000	4000	0000	0000	0000	0000
	$(2^8 \cdot 0^{16})$	$\overline{2}222$	$2\overline{222}$	0000	0000	0000	0000
$\Lambda(3)$	$(2^{12} \cdot 0^{12})$	2220	2220	2220	2000	2000	2000
	$(3^3 \cdot 1^{23})$	1113	$\overline{1113}$	$\overline{1113}$	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$
	$(2^{12} \cdot 0^{12})$	$\overline{2}222$	$\overline{2}200$	2200	2200	2200	0000
	$(4 \cdot 2^8 \cdot 0^{15})$	4000	$\overline{2}200$	$00\overline{22}$	$00\overline{22}$	$00\overline{22}$	0000
	$(5 \cdot 1^{23})$	5111	1111	1111	1111	1111	1111
	$(3^3 \cdot 1^{23})$	$\overline{1}333$	$\overline{1111}$	$\overline{1111}$	$\overline{1111}$	$\overline{1111}$	$\overline{1111}$
$\Lambda(4)$	$(2^{16} \cdot 0^8)^+$	2220	2220	2220	2220	2220	2000
	$(3^5 \cdot 1^{19})$	1113	$\overline{1113}$	$\overline{1113}$	$\overline{1113}$	$\overline{1113}$	$1\overline{111}$
	$(2^{16} \cdot 0^8)^-$	$\overline{22}20$	2220	2220	2220	2220	2000
	$(3^5 \cdot 1^{19})$	$11\overline{31}$	$\overline{1113}$	$\overline{1113}$	$\overline{1113}$	$\overline{1113}$	$1\overline{111}$
	$(4^4 \cdot 0^{20})$	4000	4000	4000	4000	0000	0000
	$(2^{16} \cdot 0^8)^-$	$\overline{2}222$	$2\overline{222}$	$2\overline{222}$	$2\overline{222}$	0000	0000
	$(4^2 \cdot 2^8 \cdot 0^{14})$	2220	2004	2004	2000	2000	$\overline{2}000$
	$(3^5 \cdot 1^{19})$	1113	$\overline{133}1$	$\overline{133}1$	$1\overline{111}$	$1\overline{111}$	$\overline{1}111$
	$(4 \cdot 2^{12} \cdot 0^{11})$	2220	2220	2220	2000	2000	$\overline{2}004$
	$(3^5 \cdot 1^{19})$	1113	$\overline{1113}$	$\overline{1113}$	$1\overline{111}$	$1\overline{111}$	$\overline{311}3$
	$(5 \cdot 3^2 \cdot 1^{21})$	5111	1111	$3\overline{111}$	$3\overline{111}$	$\overline{1111}$	$\overline{1111}$
	$(3^5 \cdot 1^{19})$	$\overline{1}333$	$\overline{1111}$	$3\overline{111}$	$3\overline{111}$	1111	1111
	$(6 \cdot 2^7 \cdot 0^{16})$	$62\overline{2}0$	2000	2000	2000	2000	2000
	$(5 \cdot 3^2 \cdot 1^{21})$	$\overline{3}153$	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$	$1\overline{111}$
	$(8 \cdot 0^{23})$	8000	0000	0000	0000	0000	0000
	$(4^4 \cdot 0^{20})$	$\overline{4}444$	0000	0000	0000	0000	0000

Table 7: Fusion of N-orbits under Co_0

Proof Firstly, we will show that the listed classes do not overlap. Suppose we have $x, y \in \Lambda$ of type ≤ 4 which are congruent (mod 2Λ), and with $x \neq \pm y$. Then $x - y$ and $x + y$ are non-zero in 2Λ; say $x - y = 2u$, $x + y = 2v$, $u, v \in \Lambda$. Now u and v are non-zero, so have type ≥ 2. Hence $x \pm y$ has type ≥ 8. But then $128 \leq (x \pm y).(x \pm y) = x.x + y.y \pm 2(x.y) \leq 128 \pm 2(x.y)$, whence $x.y = 0$ (so x and y are orthogonal) and $x.x = y.y = 64$ (so $x, y \in \Lambda(4)$). So x and y are in the same co-ordinate frame of $\Lambda(4)$, and so the classes do not overlap.

Secondly, note that the number of classes is:

$$1 + \frac{|\Lambda(2)|}{2} + \frac{|\Lambda(3)|}{2} + \frac{|\Lambda(4)|}{48} \tag{36}$$

which is precisely $2^{24} = |\Lambda/2\Lambda|$, by direct calculation from Table 5 on page 36. So these are precisely the equivalence classes (mod 2Λ). ■

Theorem 7.3.7 $|Co_0| = 8315553613086720000 = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$

Proof We observe:

- The orbit of the vector $8e_\infty$ in Co_0 is $\Lambda(4)$, by Theorem 7.3.5.
- The orbit of the vector $8e_\infty$ in N has size 48, and consists of the vectors $\pm 8e_i$ for each $i \in \Omega$, and any element of Co_0 taking $8e_\infty$ to one of these is in N, by Lemma 7.3.2.
- The stabilizers of $8e_\infty$ in N and Co_0 are the same, also by Lemma 7.3.2

Thus by the Orbit-Stabilizer Theorem, we have:

$$|Co_0| = |\Lambda(4)| \cdot \frac{|N|}{48} \tag{37}$$

By Table 5, we calculate $|\Lambda(4)| = 398034000$. By Corollary 7.3.3, we know $N = 2^{12}M_{24}$, and from Table 4 on 28, we know $|M_{24}| = 24 \times 23 \times 22 \times 21 \times 48$. Thus equation (37) gives the result. ■

7.4 Some sporadic groups involved in Co_0

Co_0 has centre $Z = \{\pm I\}$, where I is the (24×24) unit matrix. We define $Co_1 = Co_0/Z$.

We define Co_2 to be the stabilizer in Co_0 of a vector $x_2 \in \Lambda(2)$. Because of the transitivity of Co_0 on $\Lambda(2)$, the choice of x_2 does not matter. Similarly, we define Co_3 to be the stabilizer of a vector $x_3 \in \Lambda(3)$.

The groups Co_1, Co_2 and Co_3 are called the *Conway groups* after their discoverer. They are sporadic simple groups; a proof of their simplicity is given in [Asc94] chapter 9. We have enough information to determine their orders.

Theorem 7.4.1 *We have:*

- $|Co_1| = 2^{21}3^9 5^4 7^2 11 \cdot 13 \cdot 23 = 4157776806543360000$
- $|Co_2| = 2^{18}3^6 5^3 7 \cdot 11 \cdot 23 = 42305421312000$
- $|Co_3| = 2^{10}3^7 5^3 7 \cdot 11 \cdot 23 = 495766656000$

Proof The orders are respectively $|Co_0|/2$, $|Co_0|/|\Lambda(2)|$ and $|Co_0|/|\Lambda(3)|$. We know the order of Co_0 from Theorem 7.3.7, and we can calculate

$$|\Lambda(2)| = 196560$$

$$|\Lambda(3)| = 16773120$$

from Table 5 on page 36. ■

There are other sporadic groups involved in Co_0. It is possible to show that Co_0 is transitive on vectors of type 5 and 7. The stabilizer of a vector of type 5 is $McL.2$ (where McL is a sporadic simple group with order $|Co_0|/|\Lambda(5)|$ discovered by McLaughlin). The stabilizer of a vector of type 7 is the Higman-Sims sporadic group HS, with order $|Co_0|/|\Lambda(7)|$. Details are given in [Con99] and [Asc94].

References

[AS68] A. Adrian Albert and Reuben Sandler. *An introduction to finite projective planes.* Holt, Rinehart and Winston, 1968.

[Asc94] Michael Aschbacher. *Sporadic groups.* Cambridge University Press, 1994.

[Cha95] Robin J. Chapman. An elementary proof of the simplicity of the Mathieu groups M_{11} and M_{23}. *Amer. Math. Monthly*, 102(6):544–545, June-July 1995.

[Con99] J. H. Conway. Three lectures on exceptional groups. In *Sphere Packings, Lattices and Groups*, pages 267–298. Springer-Verlag, 3rd edition, 1999.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups.* Springer-Verlag, 3rd edition, 1999.

[DM96] John D. Dixon and Brian Mortimer. *Permutation Groups.* Springer, 1996.

[Gri98] Robert L. Griess, Jr. *Twelve Sporadic Groups.* Springer, 1998.

[HP85] D. R. Hughes and F. C. Piper. *Design Theory*, chapter 8. Cambridge University Press, 1985.

[Iva99] A. A. Ivanov. *Geometry of Sporadic Groups I: Petersen and tilde geometries*, chapter 2. Cambridge University Press, 1999.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[Rot84] Joseph J. Rotman. *The Theory of Groups: an Introduction.* Allyn and Bacon, Inc., 3rd edition, 1984.

[Sol95] Ron Solomon. On finite simple groups and their classification. *Notices of the A.M.S.*, pages 231–239, February 1995.