Mathematics and Music: The Mathieu Group $M_{12}$

Emma Ross

Year 4 Project
School of Mathematics
University of Edinburgh
January 2011
Abstract

Despite falling into seemingly contrasting disciplines of art and science, music lends itself surprisingly well to mathematical interpretation and understanding. The appearance of symmetry and repetition of some central theme is extremely common in musical composition and group theory provides us with the ideal tools with which to study this. This project finds its roots in the music composed by Oliviér Messiaen which owes most of its structure to the sporadic group $M_{12}$. Some context and motivation for studying this exceptional group opens the discussion. The majority of the material covered attempts to build an understanding of the construction of $M_{12}$ - Chapters 2 to 4 exploring in particular detail its relationship with Steiner systems and coding theory. Some interesting properties of the group are presented in the penultimate chapter before returning to Messiaen’s music to close the project. Analysis of one of his pieces in the final chapter serves to demonstrate the mathematics at work in the structuring of music.

This project report is submitted in partial fulfilment of the requirements for the degree of MA (Hons) Mathematics.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>ii</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1 The Mathieu Groups: Historical and Mathematical Context</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Musical Motivation</td>
<td>3</td>
</tr>
<tr>
<td>2 Mongean Shuffles</td>
<td>5</td>
</tr>
<tr>
<td>3 Steiner Systems</td>
<td>7</td>
</tr>
<tr>
<td>3.1 Definition and Properties of Steiner Systems</td>
<td>7</td>
</tr>
<tr>
<td>3.2 Constructing S(5,6,12) by Extension</td>
<td>10</td>
</tr>
<tr>
<td>3.2.1 The Affine Plane</td>
<td>10</td>
</tr>
<tr>
<td>3.2.2 Extending $AG_2(3)$</td>
<td>11</td>
</tr>
<tr>
<td>3.2.3 Extending $W_{10}$</td>
<td>14</td>
</tr>
<tr>
<td>3.2.4 Extending $W_{11}$</td>
<td>16</td>
</tr>
<tr>
<td>3.3 Permuting the Points of the Projective Line</td>
<td>18</td>
</tr>
<tr>
<td>4 S(5,6,12), the MINIMOG and the ‘Kitten’</td>
<td>19</td>
</tr>
<tr>
<td>4.1 The MINIMOG Description</td>
<td>19</td>
</tr>
<tr>
<td>4.1.1 Error Correcting Codes</td>
<td>20</td>
</tr>
<tr>
<td>4.1.2 The MINIMOG and Hexads</td>
<td>22</td>
</tr>
<tr>
<td>4.2 The ‘Kitten’</td>
<td>24</td>
</tr>
<tr>
<td>5 Properties of $M_{12}$</td>
<td>28</td>
</tr>
<tr>
<td>6 $M_{12}$ in Music</td>
<td>30</td>
</tr>
<tr>
<td>6.1 Ile De Feu 2: A Breakdown</td>
<td>31</td>
</tr>
<tr>
<td>6.1.1 Pitch</td>
<td>31</td>
</tr>
<tr>
<td>6.1.2 Note Duration</td>
<td>31</td>
</tr>
<tr>
<td>6.2 Messiaen’s <em>Charm of Impossibilities</em></td>
<td>32</td>
</tr>
<tr>
<td>A Cols and Tets</td>
<td>34</td>
</tr>
<tr>
<td>B Crosses and Squares</td>
<td>35</td>
</tr>
<tr>
<td>C Kitten in the Shuffle Labelling</td>
<td>36</td>
</tr>
<tr>
<td>D Excerpt from <em>Ile De Feu 2</em></td>
<td>37</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Olivier Mesiaen’s deliberate and extensive use of a certain selection of permutations in his 1950’s music motivates the content of this project. The French composer used permutations which were later discovered to form the Mathieu group $M_{12}$ - one of the first sporadic groups to be discovered by Emile Mathieu in 1861 and 1873. In this opening chapter the Mathieu groups put into some context in the history and understanding of group theory before narrowing focus onto the group $M_{12}$ in particular.

1.1 The Mathieu Groups: Historical and Mathematical Context

We first clarify the notation adopted in this project. If $G$ is a group acting on set $\Omega$ then $\alpha^g$ denotes the action of element $g \in G$ on $\alpha \in \Omega$, while $G_\alpha = \{g \in G | \alpha^g = \alpha\}$ defines the stabilizer of $\alpha$. To put the Mathieu groups into context within the study of group theory, we recall two key definitions from algebra.

Definition 1. \[2\] A subgroup $N$ of a group $G$ is normal in $G$ if it is invariant under conjugation - that is, for each element $n \in N$ and each $g \in G$, the element $gng^{-1} \in N$.

Definition 2. \[19\] A finite simple group is a nontrivial finite group with no proper normal subgroups, i.e. its only normal subgroups are the trivial group and the group itself.
Just as prime numbers cannot be factorized into smaller numbers, finite simple groups cannot be broken down in terms of smaller groups. We can interpret the finite simple groups intuitively as the building blocks of all finite groups. One of the greatest achievements of 20th century mathematics, the Classification of Finite Simple Groups Theorem (given below), succeeds in classifying all of the infinitely many finite simple groups into just a handful of families.

**Theorem 3.** Every finite simple group is isomorphic to one of the following groups;

- A cyclic group with prime order;
- An alternating group of degree at least 5;
- A classical group;
- An exceptional group of Lie type; or
- One of 26 sporadic simple groups.

Details of these categories and the groups which they contain can be found in most texts dealing with the finite simple groups - in particular the above is quoted from Wilson’s book[27].

This classification means that many complex problems relating to finite groups can be broken down into much simpler problems in terms of these core groups. Reaching a completed proof of the theorem was a vast and complicated task however. Counted as the longest in history, it spans over one hundred authors and even more journals and is evidently bypassed here.

Refocusing our aim, it is the latter of the 5 categories - those ‘exceptions to the rule’ which we call the Sporadic Groups - into which the Mathieu Groups fall. These five groups (\(M_{11}, M_{12}, M_{22}, M_{23}, M_{24}\)) form their own subfamily as groups of permutations of a certain number of objects - dictated by the subscript in their name. Émilé Mathieu first introduced these Groups in 1861 and 1873 in two papers published in the *Journal de Mathematiques Pures et Appliquees*. As the first Sporadic Groups to be discovered, this was some achievement as no more
were identified for around a century - the next being found by Zvonimir Janko in 1965.

1.2 Musical Motivation

Useful in the closing chapter of this project but also to providing an early understanding of the motivations behind paying particular attention to $M_{12}$, we note the relevance of this group when considering the interface between mathematics and music. Although it is a peculiar coincidence that Messiaen featured permutations from such a remarkable group in his music, it is no coincidence that it is $M_{12}$ over the other four Mathieu Groups that he was working in harmony with. The modern western musical scale can be split up into exactly twelve distinct pitch classes. We demonstrate this by first numbering the twelve notes of the scale given below.

![Figure 1.1: Assigning integer labels to each musical note](image)

Assigning numbers to the notes makes spotting the working of modulo 12 arithmetic in the musical scale a much simpler task. Progressing rightwards along the scale in Figure 1.1 the notes become higher in pitch but having reached note 11 we return to 0 in the numbering and start again. This reflects a key property of our musical scale; the note 0 is equivalent to note 12, as well as to note 24 and so on (likewise in the negative direction). Notes equivalent in modulo 12 arithmetic are distinguishable only by pitch - that is note 12 is simply a higher pitched version of 0 while 24 is doubly higher in pitch compared to 0 and so on. It is natural then to consider permutations of these twelve classes of ‘equivalent’ notes and hence the group $M_{12}$. Numbering the notes as in Figure 1.1 we consider the permutation of a set of 12 integers which generate different orderings of notes to give new melodic phrases. The first labelling shown (A) gives emphasis to the
musical convention of considering C (numbered 0) to be the central note in the scale. The second numbering is one which we will return to in the final chapter as that with which Messiaen begins his process of composition.
Chapter 2

Mongean Shuffles

The Mathieu Group $M_{12}$ can be constructed in numerous ways which tap into a variety of areas of mathematics. Demonstrating that $M_{12}$ can be understood via simple card shuffling, we begin with perhaps the least technically involved construction. Serving to initiate an intuitive understanding of the group, this construction comprises a brief second chapter.

Diaconis, Graham and Kantor discovered that $M_{12}$ can be generated by just two permutations\[14\]. Expressed below in both two-line notation and cycle notation we denote these generating permutations $P_I$ and $P_O$.

\[
P_I = \begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
5 & 6 & 4 & 7 & 3 & 8 & 2 & 9 & 1 & 10 & 0 & 11
\end{pmatrix}
= (0 \ 5 \ 8 \ 1 \ 6 \ 2 \ 4 \ 3 \ 7 \ 9 \ 10)(11)
\]

(2.1)

\[
P_O = \begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
6 & 5 & 7 & 4 & 8 & 3 & 9 & 2 & 10 & 1 & 11 & 0
\end{pmatrix}
= (0 \ 6 \ 9 \ 1 \ 5 \ 3 \ 4 \ 8 \ 10 \ 11)(2 \ 7)
\]

(2.3)

Benson however, provides a more memorable diagrammatic representation\[4\]. $P_I$ and $P_O$ are given in respective order below but beware of Benson’s practice of counting from 1 to 12. A numbering from 0 to 11 is adopted in this project,
consistent with the integers modulo 11. Diaconis, Graham and Kantor called

these permutations Mongean Shuffles. The ‘shuffle’ name attached to $P_O$ and $P_I$ comes from observing that their inverse permutations are equivalent to carrying out the following shuffles described by Benson[4]. Starting with a pack of 12 cards in your left hand (numbered 0 to 11), transfer them to your right hand by placing alternately under and over the stack so far. Since we can begin by putting card 1 under or over card 0 this gives us two permutations. The latter ‘over’ shuffle (equivalent to $P_O^{-1}$) is captured by the permutation $s(t) = \min(2t, 23 - 2t)$. We already know that $M_{12} = \langle P_I, P_O \rangle$, but we can obtain an even simpler generating pair using this Mongean Shuffle. It is easily observed, particularly from Benson’s diagrams above, that swapping the order of the elements and then performing $P_I$, is equivalent to performing permutation $P_O$. We observe then that $M_{12} = \langle r, s \rangle$, where $r(t) = 11 - t$ is the order reversing permutation and $s$ is defined above.

It is obvious that $M_{12}$ is a subgroup of $S_{12}$ - the group of all permutations of 12 points.
Chapter 3

Steiner Systems

We progress now to the most documented construction of the Mathieu groups. We will see that Steiner systems - a type of block design - give us a concrete foundation on which to build an understanding of the structure of the group $M_{12}$. The combinatorial geometry of these Steiner systems will first be explored, giving us the tools to go on to construct a particularly useful Steiner system whose Automorphism Group gives us $M_{12}$.

3.1 Definition and Properties of Steiner Systems

We begin by defining the Steiner system;

**Definition 4.** [25](p. 293) A *Steiner System* $S = S(\Omega, \mathcal{B})$ is a finite set of points $\Omega$ together with a set $\mathcal{B}$ of subsets of $\Omega$ called *blocks*. These sets are such that each block in $\mathcal{B}$ has size $k$, and each subset of $\Omega$ of size $t$ lies in exactly one block.

Letting $v := \mid \Omega \mid$, $S$ is then called an $S(t,k,v)$ Steiner system and we assume $t < k < v$ to avoid trivial cases. To give a feel for what is going on in this definition the following example is presented:

**Example 5.** The *Fano Plane* in Figure 3.1 is an example of an $S(2,3,7)$ Steiner System. We have a set $\Omega$ of $v = 7$ points, together with a set $\mathcal{B}$ of 3-element blocks - represented by the 7 lines in the plane. We can see that every pair of points belongs to a unique line, i.e. every 2-element subset of $\Omega$ is in exactly one block as required.
The remainder of this section addresses the key properties of Steiner systems - called upon in the construction of $M_{12}$ later in the chapter.

Consider the problem of counting the number of blocks containing some fixed $\alpha \in \Omega$. First note that there are $\binom{v-1}{t-1}$ $t$-subsets which contain $\alpha$. We need a further $t-1$ points to complete a $t$-subset, and can choose these points freely from the remaining $v-1$ points in $\Omega$. Now, if we have a block (of size $k$) containing $\alpha$, we also know that there are $\binom{k-1}{t-1}$ $t$-subsets of the block containing $\alpha$. There are $t-1$ more elements needed to complete the subset but they must come from the $k-1$ elements left in the block. Now by Definition 4 each $t$-subset lies in a unique block so it is straightforward to conclude that there are $r := \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$ blocks containing $\alpha$. Note that this number is independent of our choice of $\alpha$.

This result leads to the following generalization:

Lemma 6. \[13\] (p. 180) Let $\lambda_i$ be the number of blocks which contain a specified $i$-subset where $1 \leq i \leq t$, then

$$\lambda_i = \binom{v-1}{t-1} = \frac{(v-i)(v-i-1)\ldots(v-t+1)}{(k-i)(k-i-1)\ldots(k-t+1)}.$$

Note: $\lambda_i$ is independent of the choice of $i$-subset.

It is clear that there are restrictions on the values of the parameters $t, k$ and $v$ - most notably that they must be such that $\lambda_i \in \mathbb{Z}$. The following theorem highlights two key relationships between the parameters of a Steiner system.

Theorem 7. \[13\] (p. 190) Consider the Steiner System defined above with each point $\alpha$ lying in exactly $r$ blocks. The following properties hold:
1. \( bk = vr; \)

2. \( v \leq b \text{ and } k \leq r \) (Fisher’s Inequality).

Proof. 1. Let us count the number \( p \) of pairs \((\alpha, \beta)\) such that \( \alpha \in \beta \). We have \( b \) different blocks to choose from and \( k \) choices of point within those blocks so we have \( p = bk \). Alternatively, observe that we have \( v \) different choices of \( \alpha \) and \( r \) blocks containing this \( \alpha \) so that \( p = vr \).

2. Note that we can describe the structure of an \( S(t,k,v) \) Steiner system with \( b \) blocks using a \( v \times b \) incidence matrix \( M \). Each \( \alpha_i \in \Omega \) is identified with a column and each block \( \beta_j \in \mathcal{B} \) with a row (where \( 1 \leq i \leq v \) and \( 1 \leq j \leq b \)). Then \( M \) is such that

\[
M_{(i,j)} = \begin{cases} 
1 & \text{if } \alpha_i \in \beta_j \\
0 & \text{otherwise}
\end{cases}
\]

and

\[
MM^T = \begin{cases} 
\lambda_2 & \text{when } i = j \\
2 & \text{otherwise}
\end{cases}
\]

The second relation becomes clear when we notice that the \((i,j)^{th}\) element of \( MM^T \) is \( M_{(i,j)} \times M_{(i,j)} \) which is the number of blocks containing both \( \alpha_i \) and \( \alpha_j \). If \( i = j \) this is clearly just the number of times \( \alpha_i \) appears in a block - a value already defined and denoted by \( r \). When \( i \neq j \) we simply apply Lemma 6 with \( i = 2 \) to get \( \lambda_2 \). Using Lemma 6 again with our assumption that \( t < k < v \) we can show that \( r > \lambda_2 \) and hence that

\[
\det(MM^T) = (v + \lambda_2(r - 1))(r - 1)^{v-1} \neq 0.
\]

This means \( MM^T \) is non-singular and thus has full rank so that \( v = \text{rank}(MM^T) \leq \text{rank}(M) \leq b \). We then conclude \( k \leq r \) using part 1.

\[\square\]

The method of construction of the Steiner systems in the subsequent section relies heavily on a mechanism for finding new systems from old by adding or removing points from \( \Omega \) and defining new blocks. Given \( S = S(\Omega, \mathcal{B}) \) (an \( S(t,k,v) \) Steiner system) for any point \( \alpha \) we can form a new Steiner system \( S_\alpha = S(\Omega', \mathcal{B}') \) with \( \Omega' := \Omega \setminus \{\alpha\} \) and \( \mathcal{B}' := \{\beta \setminus \{\alpha\} \mid \beta \in \mathcal{B} \text{ and } \alpha \in \beta\} \). \( S_\alpha \) is called the contraction of \( S \) at \( \alpha \) and is an \( S(t - 1,k - 1,v - 1) \) Steiner system. We can
refer to $S$ as the *extension* of $S_{2n}$ though, unlike contractions, extensions are not always possible [13] (p. 184).

### 3.2 Constructing $S(5,6,12)$ by Extension

The aim of this section is to build by extension the Steiner systems whose Automorphism groups give us the small Mathieu Groups $M_{11}$ and $M_{12}$. This process begins with the Affine geometry $AG_2(3)$ and finds its end with $S(5,6,12)$ whose Automorphism group yields the Mathieu group $M_{12}$. The construction is based largely on pages 184-192 of Dixon and Mortimer [13].

#### 3.2.1 The Affine Plane

Let $\mathbb{F}_q$ be the finite field of $q$ elements with $q$ a prime power. We denote the finite affine space of dimension 2 over this field with $A := AG_2(q)$ where $q$ defines the *order* or the number of points per line in $A$. The following properties of the affine plane $A$ come as lemmas and corollaries in Batten[3] (p. 70) and Dixon and Mortimer’s [13] (p. 82-84) books:

1. $A$ has $q^2$ points and $q^2 + q$ lines;
2. Any point $p$ in $A$ is on $q + 1$ lines;
3. Any point $p$ not on a line $l$ lies on another line $l'$ which misses $l$ (i.e. $l$ and $l'$ are parallel);
4. There are $q + 1$ parallel classes in $A$;
5. Each line $l$ in $A$ is parallel to $q$ lines (so that each parallel class contains $q$ lines);
6. Any 2 points $p' \neq p$ in $A$ lie on a unique line.

The properties above mean that we can view the Affine plane as an $S(t,k,v)$ Steiner system whose parameter values we will now find. Let the set of points $\Omega$ from Definition [4] be the set of $v = q^2$ points from the 2-dimensional vector space...
over field $\mathbb{F}_q$. Then let the set of blocks $\mathcal{B}$ be the set of $k = q^2 + q$ affine lines. Now by property 6 above we have that any 2 points lie in a unique block so we deduce that $AG_2(q)$ is in fact an $S(2, q^2 + q, q^2)$ Steiner system.

Substituting $q = 3$ into the above result, we recognize $AG_2(3)$ as an $S(2,3,9)$ Steiner system. $\Omega$ contains 9 points in the 2-dimensional vector space over $\mathbb{F}_3 = \{0, 1, 2\}$. Spotting the underlying Steiner system is helped by the graphic representation of $AG_2(3)$ in Figure 3.2 (taken from Afanas’ev[1]).

![Figure 3.2: The Affine Plane of order 3: S(2,3,7)](image)

We note (for future reference) that the lines of this finite plane can be grouped into classes of parallel lines. Taking the bottom left point seen in Figure 3.2 as the origin $(0,0)$, the parallel classes are described in Table 3.1 where each row of points represents the line which joins them. Note the existence of $q + 1 = 4$ classes each containing $q = 3$ lines as predicted by properties 4 and 5 above.

<table>
<thead>
<tr>
<th>Vertical Lines</th>
<th>Horizontal Lines</th>
<th>+ gradient</th>
<th>- gradient</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(0,0),(0,1),(0,2)$</td>
<td>$(0,0),(1,0),(2,0)$</td>
<td>$(0,0),(1,1),(2,2)$</td>
<td>$(0,0),(1,2),(2,1)$</td>
</tr>
<tr>
<td>$(1,0),(1,1),(1,2)$</td>
<td>$(0,1),(1,1),(2,1)$</td>
<td>$(0,1),(1,2),(2,0)$</td>
<td>$(0,1),(1,0),(2,2)$</td>
</tr>
<tr>
<td>$(2,0),(2,1),(2,2)$</td>
<td>$(0,2),(1,2),(2,2)$</td>
<td>$(0,2),(1,0),(2,1)$</td>
<td>$(0,2),(1,0),(2,0)$</td>
</tr>
</tbody>
</table>

Table 3.1: The Parallel classes of $AG_2(3)$

**Theorem 8.** Up to isomorphism, $AG_2(3)$ is the unique $S(2,3,9)$ Steiner system.

**Proof.** The proof of this result comes as a consequence of the observations made above and can be found in Dixon and Mortimer’s book[13](p. 186).

3.2.2 Extending $AG_2(3)$

The aim of this section is to extend the $S(2,3,9)$ Steiner system to an $S(3,4,10)$ Steiner system which we will denote $W_{10}$. Recall that to do so we add a new point
\( \alpha \) and look for new blocks which fit the requirements of an S\((3,4,10)\) system. Let us first seek out the characteristics that S\((3,4,10)\) must hold. We know immediately from the definition of a Steiner system that each 3-subset of points will lie in a unique block of size 4. With parameters \( t = 3, \ k = 4 \) and \( v = 10 \), the definition of \( r \) from Section 3.1 tells us that each point must be contained in \( r = 12 \) blocks. Part 1 of Theorem 7 allows us to conclude that there will be \( b = 30 \) blocks in \( W_{10} \).

To find the desired blocks, let us first assume that we already have an S\((3,4,10)\) Steiner system. By the definition of a contraction of a Steiner system (given at the end of Section 3.1), if we remove a point \( \alpha \) from S\((3,4,10)\) we will have an S\((t-1, k-1, v-1)\) system which by Theorem 8 is isomorphic to \( AG_2(3) \). From this we see that a block in S\((3,4,10)\) containing \( \alpha \) must be of the form \( \Lambda \cup \alpha \) where \( \Lambda \) denotes a block (line) in \( AG_2(3) \). Since we found that there were 12 such \( \Lambda \), these unions form 12 of the blocks of \( W_{10} \) - accounting for those containing 3 collinear points and those containing \( \alpha \). We calculated however that we need 30 blocks and so there must be a 18 further blocks consisting of four points in \( AG_2(3) \) which do not contain \( \alpha \) or any 3 collinear points (i.e. which meet any \( \Lambda \) in at most 2 points) since all such blocks are already accounted for in \( \Lambda \cup \alpha \). We will call such 4-sets quadrangles, denoted \( \Xi \), of which there are 54\([13]\)(p. 186). Note that looking for such blocks is equivalent to looking for a set of 18 quadrangles to cover the set of 72 triangles of \( AG_2(3) \) one each\([13]\)(p. 186).

**Theorem 9.** There are 3 sets of 18 quadrangles of \( AG_2(3) \) such that each triangle of \( AG_2(3) \) is contained in a unique quadrangle from each set.

**Proof.** To define the three sets referred to in the theorem we note some properties of quadrangles from \( AG_2(3) \). Each pair of points in a quadrangle \( \Xi \) can be joined by a line in \( \Xi \) of which there are six. Each line from this set of 6 must belong to one of the 4 parallel classes of Table 3.1 so there must be 2 pairs of parallel lines in the set. Naturally then, we can associate to each quadrangle a pair \( \{x, y\} \) (called the type of \( \Xi \)) where \( x \) and \( y \) are those parallel classes which contain such a pair. Let us represent the set of 4 parallel classes of \( AG_2(3) \) by \( a, b, c, d \). We
can break this set into two pairs in three different ways; \(ab | cd, ac | bd, ad | bc\). We can now define

- \(S_1\) = the set of all quadrangles with type \(\{a, b\}\) or \(\{c, d\}\)
- \(S_2\) = the set of all quadrangles with type \(\{a, c\}\) or \(\{b, d\}\)
- \(S_3\) = the set of all quadrangles with type \(\{a, d\}\) or \(\{b, c\}\),

corresponding to the three partitions above. We state without proof the result that \(Aut(AG_2(3))\) acts on the set of parallel classes in the same way in which the symmetric group \(S_4\) acts on a set of 4 points. This leads to the conclusion that the 54 quadrangles in \(AG_2(3)\) are split evenly into the sets \(S_i\) (\(i = 1, 2, 3\)) containing 18 quadrangles each.

We claim that each triangle belongs to a unique quadrangle in each of these sets \(S_i\). By symmetry it is enough to prove each triangle belongs to a unique quadrangle in just one \(S_i\). We will use (wlog) \(S_1\). Consider a triangle \(T\) and observe that each of its three sides lie in different parallel classes so that one class, say \(d\), is not represented. We can add a point \(p\) to our triangle to obtain a quadrangle. Again, all 3 lines through new point \(p\) must belong to different parallel classes. Since \(d\) was not in the original triangle and can only be represented once in the lines through \(p\) we know that \(d\) appears less than twice in this quadrangle. Consequentially, we know by the definition of the type of a quadrangle above that \(T\) cannot be contained in any quadrangle of type \(\{c, d\}\). We can show however that \(T\) is contained in a quadrangle of type \(\{a, b\}\). Labelling the vertices of the triangle \(v_1, v_2\) and \(v_3\), let the line connecting \(v_1\) to \(v_2\) be of class \(a\) and the line \(v_1\) to \(v_3\) be of class \(b\) (wlog). Since the line of class \(a\) through \(v_3\) and the line of class \(b\) through \(v_2\) are clearly not parallel, they must intersect at a point, say \(p^*\). Then \(\Xi = \{v_1, v_2, v_3, p^*\}\) is the unique quadrangle in \(S_1\) containing \(T\) which we are searching for.

\[\square\]

It can be proved that these \(S_i\) (\(i = 1, 2, 3\)) are the only sets of 18 quadrangles with this property, a proof for which can be found in Dixon and Mortimer’s book [13] (p. 188).
Looking at our 2 classes of blocks - those constructed with quadrangles and those of the form $\Lambda \cup \alpha$ - we see that we are done. Consider any 3 collinear points. By the properties of $S(2,3,9)$ we know that any 2 or more points in $AG_2(3)$ belong to a unique block $\Lambda$ and so any 3 collinear points must belong to a unique 4-block $\Lambda \cup \alpha$. Now for non-collinear points, although Theorem 9 means we have 3 choices for blocks not containing $\alpha$, we know that in each case any triangle (set of 3 non-collinear points) is contained in one unique block of 4. Hence we have satisfied the properties of an $S(3,4,10)$ Steiner system with the above as our blocks.

We have shown that $S(3,4,10)$ is a one-point extension of $S(2,3,9) \cong AG_2(3)$ and in fact it can be shown that all Steiner systems which are one-point extensions of $AG_2(3)$ are isomorphic\[13\](p. 188). The following theorem concludes this subsection:

**Theorem 10.** Up to isomorphism, there is a unique $S(3,4,10)$ Steiner system denoted $W_{10}$

*Proof.* Let $W$ be an $S(3,4,10)$ Steiner system and $\alpha$ a point in $W$. Contracting $W$ at $\alpha$ by removing the point $\alpha$ and those blocks containing it, we obtain an $S(2,3,9)$ Steiner system which by Theorem 8 is the affine geometry $AG_2(3)$. Since $W$ is a one-point extension of $AG_2(3)$ it is determined up to isomorphism and we call it $W_{10}$. \qed

### 3.2.3 Extending $W_{10}$

It is important to bear in mind the final aim of this process of extension - that is to reach the $S(5,6,12)$ Steiner system and reveal its close relationship with $M_{12}$. In this section we will extend $W_{10} = S(3,4,10)$ to $W_{11} = S(4,5,11)$. Note that we denote these systems $W_n$ as they coincide with Ernst Witt’s *Witt Geometries*. We advance just as before - adding a point $\alpha$ to $W_{10}$ and finding those blocks which give us an $S(4,5,11)$ Steiner system.

Again, we begin by assuming we already have a $S(4,5,11)$ Steiner system which we call $W$. Consider 2 of its points $\alpha$ and $\beta$ which are not in $AG_2(3)$. By construction the contractions $S_\alpha$ and $S_\beta$ are both $S(3,4,10)$ and isomorphic as one-point extensions of $AG_2(3)$. This means that we can understand the set of
points in $W$ as the points in $AG_2(3)$ along with $\alpha$ and $\beta$. Just as we observed previously, the blocks of $W$ are of one of the following forms:

$$\Lambda \cup \{\alpha, \beta\}, \quad \Xi_2 \cup \{\alpha\}, \quad \Xi_1 \cup \{\beta\},$$

where $\Xi_1$ denotes a quadrangle from $S_1$ and $\Xi_2 \in S_2$.

Consider those blocks containing neither $\alpha$ nor $\beta$ which must lie in $AG_2(3)$. We note without proof that any set of five points in $AG_2(3)$ contains a quadrangle, so the remaining blocks must contain quadrangles from $S_3$. By the definition of the Steiner system however each set of 4 must lie in just one block so any quadrangles found in the blocks above involving $S_1$ or $S_2$ are already accounted for and so cannot feature in the remaining blocks. To conclude the nature of the remaining blocks we require the following properties[13](p. 187):

1. For any quadrangle $\Xi$ there is a unique point $\delta$ outside of $\Xi$ which lies on two distinct lines of $\Xi$, which we call the diagonal point.

2. There exists a unique quadrilateral $\Xi^*$ disjoint from $\Xi$ for which $\Xi^*$ and $\Xi$ share the same diagonal point.

3. If $\Xi^*$ has type $\{a,b\}$ then $\Xi$ has type $\{c,d\}$, i.e. the parallel classes associated with $\Xi^*$ have none in common with that of $\Xi$.

We see then that each of the blocks of $W$ which do not contain $\alpha$ or $\beta$, i.e. which are disjoint from $\{\alpha, \beta\}$ must be of from $\Xi_3 \cup \{\delta\}$ where $\Xi_3$ is a quadrangle from $S_3$ and $\delta$ is the diagonal point of $\Xi_3$.

This argument is reversed in Dixon and Mortimer’s[13] book to prove the existence of a $S(4,5,11)$ system:

**Theorem 11.** Up to isomorphism there is a unique $S(4,5,11)$ Steiner system, denoted $W_{11}$.

**Proof.** The $S(4,5,11)$ system is constructed, letting $AG_2(3) \cup \{\alpha, \beta\}$ be the points of $W$. Discussed in the preamble to this theorem, the blocks of $W$ are of the
following forms:

\[ \Lambda \cup \{ \alpha, \beta \}; \Xi_1 \cup \{ \alpha \}; \Xi_2 \cup \{ \beta \} \text{ or } \Xi_3 \cup \{ \delta \} \]

Our previous work tells us that there are 12 blocks involving \( \Lambda \) and 18 of each of the remaining forms involving quadrangles. We have 66 blocks in total then but by our definition of \( r \) coupled with part [1] of Theorem [7] - or alternatively simple counting theory - we have \(|\mathcal{B}| = \binom{11}{5}/\binom{5}{5} = 66 \) for a \( S(4,5,11) \), so we have all the blocks we need. To prove \( \mathcal{B} \) satisfies the conditions for an \( S(4,5,11) \) Steiner system then, it suffices to show that each set of 4 is in at least one block. The argument used to prove this exploits the properties of the blocks and of the parallel classes of \( AG_2(3) \). The details of this can be found in Dixon and Mortimer [13] (p. 190-191) along with a proof of the uniqueness of \( W \) based on the uniqueness \( W_{10} \) and \( AG_2(3) \).

\[ \square \]

### 3.2.4 Extending \( W_{11} \)

The final step of this process - extending \( W_{11} \) to \( W_{12} := S(5,6,12) \) - is a simple repetition of previous methods. Let \( \mathcal{C}_i \) denote the subsets of \( AG_2(3) \) of the form \( \Xi \cup \{ \delta \} \), i.e. the latter three forms of block described in the previous section. Suppose now that we already have \( W \), a \( S(5,6,12) \) Steiner system which contains points \( \alpha, \beta \) and \( \gamma \). The one-point contractions \( W_\alpha, W_\beta \) and \( W_\gamma \) can all be constructed using the \( \mathcal{S}_i \) and \( C_i \) just as in the previous construction of \( W_{11} \) (since \( W_{11} \) it is unique up to isomorphism). The set of points of \( W \) consists of points in \( AG_2(3) \cup \{ \alpha, \beta, \gamma \} \). Based on similar principals from our previous construction work we note that blocks which contain points from \( \{ \alpha, \beta, \gamma \} \) will be in one of the following forms:

1. \( \Lambda \cup \{ \alpha, \beta, \gamma \} \)
2. \( \Xi_1 \cup \{ \beta, \gamma \} \) where \( \Xi_1 \) is a quadrangle from \( \mathcal{S}_1 \)
3. \( \Xi_2 \cup \{ \alpha, \gamma \} \) where \( \Xi_2 \) is a quadrangle from \( \mathcal{S}_2 \)
4. \( \Xi_3 \cup \{ \alpha, \beta \} \) where \( \Xi_3 \) is a quadrangle from \( \mathcal{S}_3 \)
5. $P_1 \cup \{\alpha\}$ where $P_1 \in C_1$

6. $P_2 \cup \{\alpha\}$ where $P_2 \in C_2$

7. $P_3 \cup \{\alpha\}$ where $P_3 \in C_3$

Now there are only those blocks free of $\alpha$, $\beta$ and $\gamma$ to consider. Since we are working with an $S(5,6,12)$ Steiner system in which any 5-set is contained in only one block, the remaining blocks must not contain any of the 5 element subsets of $C_i$ ($i = 1, 2, 3$) since they already appear in the blocks described above. The remaining blocks then must not contain a quadrangle along with its diagonal point and in fact $L \cup L^*$ (where $L, L^*$ are distinct parallel lines in $AG_2(3)$) is the only form which fills our requirements.

There are 12 blocks of type 1, 18 of types 2-7 and 12 of our final type 8 above. We then have 132 blocks in total - a figure which again fits with the properties of an $S(5,6,12)$ Steiner system.

**Theorem 12.** Up to isomorphism there is a unique $S(5,6,12)$ Steiner system called $W_{12}$.

**Proof.** There is at most one way to extend $W_{11}$ to $W_{12}$ and so it remains only to show that the blocks defined above do indeed form blocks of an $S(5,6,12)$ Steiner system. The proof of this follows closely in line with that of Theorem 8 given in Dixon and Mortimer\cite{13}(p. 186).

We have reached our goal of constructing the small Witt geometry $W_{12}$ and we can now define $M_{12}$ as the automorphism group - $Aut(W_{12})$ - of the $S(5,6,12)$ Steiner system (a proof of this relationship can be found in Rotman\cite{25}(p. 304)). We understand an automorphism of a Steiner system $S(\Omega, \mathcal{B})$ as a permutation of $\Omega$ which permutes the blocks among themselves\cite{13}(p. 179). Indeed we can write

$$M_{12} := \langle g \in S_{12} : \mathcal{B}^g = \mathcal{B} \rangle .$$

This emphasises that $M_{12}$ is the stabiliser of the blocks in the steiner system, consisting of all permutations which preserve $S(5,6,12)$.
This Setiner system is exceptional in its own right - not just as a key design yielding the remarkable group $M_{12}$. There are only finitely many Steiner systems with $t > 3$ and none known with $t > 5$\cite{16}(p. 90). It should be noted that the method outlined above is certainly not the only way to forge a construction of $S(5,6,12)$ - many methods have been found for finding the blocks of this design. Hans Havelick gives a method based on contracting the $S(2,4,13)$ Steiner system, more commonly recognised as the projective plane\cite{16}(p. 90). A further method for finding the blocks of $W_{12}$ involving the projective plane is presented in a brief final section of this chapter.

3.3 Permuting the Points of the Projective Line

Consider the finite field $\mathbb{F}_{11}$ with 11 elements. The Projective Line over this field is the set of all 1-dimensional subspaces of the 2-dimensional vector space $\mathbb{F}_{11}^2$:

$$PG(1,11) = \{\infty, 0, 1, 2, \ldots, 9, 10\}.$$ 

We can obtain $M_{12}$ as a permutation group acting on these twelve elements of $PG(1,11)$.

**Definition 13.** \cite{23}(p. 07) An integer $q$ is a *quadratic residue* of $n$ if it is congruent to a perfect square modulo $n$, i.e. $q \equiv x^2(\mod n)$ for some $x \in \mathbb{Z}_n$.

Let $Q = \{0, 1, 3, 4, 5, 9\}$ namely 0 with the quadratic residues of 11, and let $L$ be the linear fractional group consisting of all permutations of the form

$$y \rightarrow \frac{ay + b}{cy + d}; \quad ad - bc = 1.$$ 

We note that $L = \langle \alpha, \beta \rangle$, (where $\alpha(y) = y+1$ and $\beta(y) = -1/y$) and is isomorphic to the Projective Linear Group $PSL(2, \mathbb{F}_{11})$ \cite{12}(p. 353). Then the set $\mathcal{L} := \{Q^x; x \in L\}$ is equivalent to $\mathcal{B}$ in the previous construction - consisting of all of the blocks of the $S(5,6,12)$ Steiner system. And so clearly we have $M_{12} := \langle g \in S_{12} ; \mathcal{L}^g = \mathcal{L} \rangle$.  

18
Chapter 4

\textbf{S(5,6,12), the MINIMOG and the ‘Kitten’}

We discovered the key role of S(5,6,12) in the understanding of $M_{12}$ in the previous chapter. Indeed much of the study of $M_{12}$ focusses on finding ways to represent and understand this useful Steiner system. Moving into computational group theory we explore alternative methods - based on the theory of error correcting codes - for finding the blocks of S(5,6,12) which we will now refer to as \textit{hexads}.

\section{The MINIMOG Description}

R.T. Curtis first derived the Miracle Octad Generator (MOG) - a $4 \times 6$ array - designed to find the octads (8-sets) of the S(5,8,24) Steiner system whose automorphism group is the largest of the Mathieu groups $M_{24}$. As an extension, (or perhaps more appropriate a ‘contraction’) of Curtis’ MOG, John Conway followed up the idea to create a $4 \times 3$ array called the MINIMOG which serves an analogous purpose with $M_{12}$ by describing the hexads of S(5,6,12). Description of the MOG goes beyond the scope of this project though it is well documented and should be recognized as the forerunner to the device which will be described in this chapter. Indeed Dutch mathematician and computer programmer Andries E. Brouwer said that ‘by far the most important structure in design theory is the Steiner system S(5, 8, 24)’ [6].
Some background in the theory of error correcting codes will first be given as it from this area of mathematics that the underlying theory for the MINIMOG originates.

4.1.1 Error Correcting Codes

This area of mathematics arose as a response to the practical problems of communicating digitally encoded information reliably. We think of messages being transmitted over some communications channel as a block of symbols from a finite field which are subject to noise and hence some level of distortion. Error correcting coding adds some redundancy to the original message so that most messages, even when distorted, can be recovered at the other end\[24\](p. 1-2).

Now a linear error correcting code $C$ is linear subspace of vector space $\mathbb{F}^n$ where ($\mathbb{F}$ is a finite field and $n \geq 0$). The elements of $C$ are the $q^k$ codewords with length $n$ where $k$ is the dimension of the code - equal to the dimension of $C$ \[15\](p. 25). It should be noted that the Galois Fields $\mathbb{F}_q$ with $q$ a power of a prime are the only finite fields $\mathbb{F}$. This section will make use of one such field - the ternary field $\mathbb{F}_3 = \{0,1,2\}$ as well as the tetracode $C_4$. We will define this code using the conventional parameters for a linear code which are given in the following definition.

**Definition 14.** \[20\](p. 8-9)

- The Hamming distance $\text{dist}(u,v)$ between two vectors $u$ and $v$ is is the number of positions in which they differ, i.e. the number of $i$ such that $u(i) \neq v(i)$ where $i = 1, \ldots, n$.

- The Minimum distance $d(C)$ of a code $C \subset \mathbb{F}^n$ is the minimum of $\text{dist}(u,v)$ where $u \neq v$.

We can then refer to an $(n,k,d)$ code which has length $n$, dimension $k$ and minimum distance $d$. This last parameter may be unknown and left out from notation though it is a useful parameter with its value determining the number of errors that can be corrected by the code\[28\]. Recognising that an $(n,k)$ code
$C$ is a vector subspace of $\mathbb{F}_q^n$ we know from linear algebra that there exists a basis of $C$ containing $k$ vectors which we can use to describe the code.

**Definition 15.** [26](p. 16) Let some basis of code $C$ consist of vectors $b_1, \ldots, b_k$. The $k \times n$ generating matrix of $C$

$$M = \begin{pmatrix}
    b_1 \\
    b_2 \\
    \vdots \\
    b_n
\end{pmatrix}
$$

has its rows as the basis vectors so that $C$ consists of all linear combinations of the rows of $M$. Note that the generating matrix of a code is not unique since choice of a basis is not unique.

We now define the code which is used in the remainder of this chapter.

**Definition 16.** [11](p. 81) The tetracode $C_4$ is a $(4, 2, 3)$ code over $\mathbb{F}_3$ (the ternary field) and has generating matrix

$$M = \begin{pmatrix}
    1 & 1 & 1 & 0 \\
    0 & 1 & -1 & 1
\end{pmatrix}.
$$

The tetracode falls into a particular subcategory of cyclic linear codes which have the property that for every codeword $(c_0, c_1, \ldots, c_{n-1})$ in $C$, $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a codeword in $C$[20](p. 188-189).

Below are all of the tetracode words [17](p. 5).

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>+</td>
<td>0</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>0</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>+</td>
<td>0</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>+</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 4.1: Tetracode Words

Associating ‘+’ with 1, ‘-’ with 2 (and 0 with 0) these are the code words of $C_4$ and form a linear code over $\mathbb{F}_3$. In a typical word $abcd$, $(a,b)$ specifies a linear function $\phi(x) = ax + b$ over $\mathbb{F}_3$ so that the leading digit defines the slope of the
word and $b = \phi(0)$ while $c = \phi(+)\text{ and } d = \phi(-)$ ([11] (p. 320), [15] (p. 360)). It is generally simpler however to remember the codewords by exploiting their symmetries. We observe that the tetracode words will be of the form

$$(a, a, a, a), (1, a, b, c) \text{ or } (2, c, b, a)$$

where $abc$ is any cyclic permutation of \{0,1,2\} ([10] (p. 359). The 4-tuples in Table 4.1 are grouped with those aligned to the left corresponding to the case where \{a,b,c\} = \{0,1,2\}. The middle and right aligned groups account for \{a,b,c\} = \{1,2,0\} and \{a,b,c\} = \{2,0,1\} respectfully. With this we can easily solve two types of error correcting problem ([10] (p. 360):

- **The 2-problem**: Complete a tetracode word from any of its 2 digits.

- **The 4-problem**: Correct a codeword given all 4 of its digits, one of which may be mistaken.

### 4.1.2 The MINIMOG and Hexads

The MINIMOG in the *shuffle labelling* is the $4 \times 3$ array to which we have assigned row labels 0, + and -, displayed in Table 4.2. This, along with our understanding

\[
\begin{array}{cccc}
0 & 6 & 3 & 0 & 9 \\
+ & 5 & 2 & 7 & 10 \\
- & 4 & 1 & 8 & 11 \\
\end{array}
\]

Table 4.2: MINIMOG in the Shuffle Labelling

of the form of tetracode words will be key in the following method for finding the hexads of the S(5,6,12) Steiner system. We define the following constructions which will be used to give a simple description of the hexads we are looking for.

We can define the *odd-man-out* for a column to be the label of the row in which the column has just one non-empty entry or alternatively just one empty entry ([11] (p. 321). If there is no such odd-man-out then a ‘?’ is written below the column. The arrays in Table A.2 of Appendix [A] have the odd-men-out written
underneath each column. We see that together they give the tetracode words seen in Table 4.1 (arranged in the same order).

**Definition 17.** \[11\] (p. 321) 
- We call a placement of 3 + signs in one column a \textit{col} (see Appendix A, Table A.1 for examples).
- We say that a \textit{tet} or \textit{tetrad} is any placement of 4 + signs (one in each column of the MINIMOG array) whose odd-man-out 4-tuple corresponds to a tetracode (see Appendix A Table A.2).

The definition which follows gives us a technique for finding hexads:

**Definition 18.** \[10\] (p. 363) The \textit{signed hexads} are those combinations of 6-sets obtained from the MINIMOG from patterns of the following forms:

1. \textit{col} - \textit{col}
2. \textit{tet} - \textit{tet}
3. \textit{col} + \textit{col} - \textit{tet}
4. \textit{col} + \textit{tet}

**Example 19.** \textit{col} - \textit{col} Example:

\[
\begin{array}{c}
+ \\
+ \\
+ \\
\end{array} 
- 
\begin{array}{c}
+ \\
+ \\
+ \\
\end{array} = 
\begin{array}{c}
+ \\
+ \\
+ \\
\end{array}
\]

Table 4.3: \textit{col} - \textit{col}

Comparing this with the MINIMOG we can pick out the corresponding entries:

\[
\begin{array}{ccc}
6 & -3 & 0 \\
5 & -2 & 7 \\
4 & -1 & 8 \\
\end{array}
\]

Table 4.4: MINIMOG array

The signed hexad is then \{-1, -2, -3, 6, 7, 10\}.

23
Lemma 20. (p. 321) If we ignore the signs, these signed hexads give us the 132 hexads of the Steiner system S(5,6,12). These turn out to be all possible hexads for which

1. the odd men out form part of a tetracode word, and

2. the distribution of symbols in the columns is not 3210 in any order.

4.2 The ‘Kitten’

The following method is an alternative for finding the hexads of S(5,6,12). A facet of the MINIMOG, it acts as a ‘pocket calculator for $M_{12}$’ (p. 353). Also derived from the construction of the MOG, it is referred to as the ‘Kitten’ (recognising that ‘mog’ is a colloquialism meaning cat).

The aim of the forthcoming device is to provide a simple way in which, given a 5-subset, the unique block or hexad in which it belongs can be easily found. The points in the plane are arranged in the ‘Kitten’ below - associated to each of the 3 points-at-$\infty$ namely 0, 1 and $\infty$. Looking into the centre of the triangle from each, we have three views from these points-at-$\infty$. These views are built up in $\mathbb{F}_2^3$ from the bottom left corner coordinate, the bottom right corner coordinate and the top left corner coordinate respectively for 0, 1 and $\infty$ (see Table 4.5).

\[
\begin{array}{cccc}
\infty & \ & \ & \\
6 & \ & \ & \\
2 & 10 & \ & \\
5 & 7 & 3 & \\
6 & 9 & 4 & 6 \\
2 & 10 & 8 & 2 & 10 \\
\end{array}
\]

Curtis’ Kitten
Table 4.5: Views from 3 points-at-\(\infty\)

The approach may seem unintuitive but its exploitation of a simple property gives us some understanding of how the system begins. We note that the extra 3 points required to complete a 3 point set to a hexad form a Steiner system S(2,3,9) (which describes \(AG_2(3)\) as we saw in Section 3.2.1). The simplicity of the method is helped along by the fact that this unique plane can be understood as the rows, columns and diagonals in a 3 \(\times\) 3 ‘knots and crosses’ game as demonstrated in Table 4.6.

Table 4.6: \(F_3\) ‘knots and crosses’

Highlighted via the above indication of the slopes of the columns, rows and diagonals, it is natural to consider rows as perpendicular to columns and slope 1 diagonals as perpendicular to slope -1 diagonals. The following terminology is the final part of the puzzle in our method for hexad construction.

**Definition 21.**

- A **cross** is a union of two perpendicular lines;
- A **square** is the complement of a cross.

Examples of crosses are marked out using filled circles in Appendix B. As their complements, the squares are the patterns of open circles.

**Theorem 22.** ([12](p. 355)) The hexads are:

1. \(\{\infty, 0, 1\}\) \(\cup\) \{any line\} (12 of these);
2. the union of two parallel lines (12 of these);
3. a point-at-$\infty$ together with a cross in the corresponding picture ($3 \times 18 = 54$ of these);

4. 2 points-at-$\infty$ with a square corresponding to the omitted point-at-$\infty$ (54 of these).

There are 132 of these hexads in total and they form the blocks of a S(5,6,12) Steiner system. It is only when a practical example is given that the simplicity and effectiveness of this tool for finding hexads is understood.

**Example 23.** 1. To find the hexad in which the 5-subset \{\infty, 1, 5, 9, 10\} lies, we look to the 0-picture (see below). Marking where these points appear in this $\mathbb{F}_3^2$ plane, we see that we can complete the square (shown adjacent) to obtain our hexad by adding the point 3. The hexad is then \{\infty, 1, 3, 5, 9, 10\}.

\[
\begin{array}{ccc}
5 & 7 & 3 \\
6 & 9 & 4 \\
2 & 10 & 8 \\
\hline
\end{array}
\]

\[
\begin{array}{ccc}
\bullet & \circ & \bullet \\
\circ & \bullet & \circ \\
\circ & \bullet & \circ \\
\hline
\end{array}
\]

0-picture

\[
\begin{array}{ccc}
\bullet & \circ & \bullet \\
\circ & \bullet & \circ \\
\circ & \bullet & \circ \\
\hline
\end{array}
\]

\begin{picture}(10,10)

square
\end{picture}

2. To find the unique hexad in which \{1, 2, 3, 4, 5\} lies, we see that the 1-picture appears as below and inclusion of point 7 completes a cross. The hexad is \{1, 2, 3, 4, 5, 7\}.

\[
\begin{array}{ccc}
5 & 7 & 3 \\
9 & 4 & 6 \\
8 & 2 & 10 \\
\hline
\end{array}
\]

\[
\begin{array}{ccc}
\bullet & \bullet & \bullet \\
\circ & \bullet & \circ \\
\circ & \bullet & \circ \\
\hline
\end{array}
\]

1-picture

\[
\begin{array}{ccc}
\bullet & \bullet & \bullet \\
\circ & \bullet & \circ \\
\circ & \bullet & \circ \\
\hline
\end{array}
\]

\begin{picture}(10,10)

cross
\end{picture}

There are of course other constructions of $M_{12}$, indeed two others using very different mathematics can be found in section 11.17 of Conway and Sloane’s book [11]. It is also important to note the exclusion of the theory of Golay codes which fall very closely in line with the material involving Steiner systems and error correcting codes. Unable to be given justice under the limitations of this project, the material discussed in the previous and current chapters is dealt with in terms of Golay codes in Conway and Sloane[11] (which also defines Golay Codes) as well as Greiss’ book[15].
Mathematical Blackjack

While the Kitten in Section 4.2 is obtained from the modulo 11 MINIMOG labelling (given in Table C.1 of Appendix C), since S(5,6,12) Steiner systems are unique up to relabellings, we can obtain an alternative kitten from the shuffle labelling (used in Section 4.1.2). This alternative Kitten is given in Table C.2 of Appendix C. We have the same concepts of squares and crosses in our new views from the 3 points-at-∞ (Table C.3 in Appendix C) with which we can find the hexads of S(5,6,12). Conway and Ryba found that a winning strategy for the game Mathematical Blackjack involves choosing a move which gives a hexad of the S(5,6,12) Steiner system in the shuffle labelling with a sum less than or equal to 21\(^{18}\). The link between the MINIMOG and card games is made in Section 11.17 of Conway and Sloane’s book\(^{11}\) while details of this particular game can be found in Joyner and Casey’s paper\(^{17}\)(p. 11-13). Magazine publisher Scientific American in fact feature an online game which demonstrates the combinatorics of hexads at play in \(M_{12}\)^{29}. 
Chapter 5

Properties of $M_{12}$

As we discovered in Chapter 1, the Mathieu Groups were the first groups found to not belong to an infinite family. Mathieu was in fact not in search of groups that were exceptional in this manner, rather he was searching for highly transitive permutation groups when he discovered the Groups which now bear his name. It was in fact after their discovery that they were proved to be simple. This section serves to highlight the key properties of $M_{12}$ which have not already been discovered through construction. Since proof of these properties largely involves substantial background work on non-elementary group theory, the reader will be provided with an idea of the origins of the proof and further reading only.

A logical start is to look at multiple transitivity since it is where Mathieu’s own search for his groups began.

Recall that a group $G$ acting on a set $\Omega$ is called transitive if it has only one orbit, that is for any $\alpha, \beta \in \Omega$ there exists a $g \in G$ such that $\alpha^g = \beta$. This idea is extended to a concept of multiple transitivity as follows:

**Definition 24.** [25](p. 250) A set $\Omega$ acted on by $G$ is $k$-transitive for $k < |G|$ if it acts transitively on the set of all $k$-tuples of distinct elements of $\Omega$. That is for such $k$-tuples $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$, $\exists g \in G$ with $gx_i = y_i$ for all $i = 1, \ldots, k$.

We also have a concept of sharp multiple transitivity:

**Lemma 25.** [8] If $G$ is $k$-transitive on $\Omega$, it is sharply $k$-transitive if there exists only one element $g$ which maps a $k$-tuple to another.
The proof of the transitivity and simplicity of $M_{12}$ will require the following definition linking $M_{11}$ and $M_{12}$:

**Definition 26.** $M_{11}$ is the point-stabilizer of $M_{12}$. We write $M_{11}= (M_{12})_{\alpha}$ where $\alpha$ is from the set of points of $W_{12}$ (i.e. those which $M_{12}$ acts upon).

**Theorem 27.** $M_{12}$ is sharply 5-transitive on the set of 12 points of $W_{12}$ and has order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 59,040$.

**Proof.** The proof of transitivity is based on the sharp 4-transitivity of $M_{11}$. Details of a method based on transitive extensions can be found in Rotman’s book[25](p.289) while a proof in line with the properties Steiner systems from Chapter 8 can found in Dixon and Mortimer[13](p. 192). The order of $M_{12}$ is found using the properties of the general affine group $AGL_2(3)$ and the Orbit Stabilizer Theorem in relation to $W_{10}, W_{11}$ and their Automorphism groups. For example, one finds that $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8$, but by the Orbit Stabilizer Theorem and Definition 26 we have $|M_{12}| = |Aut(W_{12})| = |W_{12}| \cdot |(M_{12})_{\alpha}| = 12 \cdot |M_{11}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

Much like most of the work on understanding and constructing $M_{12}$, the proof of its simplicity also comes from properties of $M_{11}$, namely its uniqueness (following from Theorem 11 in Section 3.2.3) and its simplicity (proved in numerous sources including Chapman’s paper[9]). The properties above combined with the following (given by Rotman[25]) leads to one of numerous ways to prove the simplicity of $M_{12}$.

**Lemma 28.** Let $G$ act faithfully and be $k$-transitive on a set $\Omega$ with $k \geq 4$. If $G_{\alpha}$ is simple for some $\alpha$ then $G$ is simple.

Taking $M_{12}$ to be $G$ in the above lemma, by Definition 26 we can take $M_{11}$ as $G_{\alpha}$ which we already know is simple. By Theorem 27 we know that $M_{12}$ is 5-transitive so $k = 5 \geq 4$ and so $G = M_{12}$ is simple.

Having come to the end of our discussion of $M_{12}$ we have seen that the Mathieu Groups are truly remarkable finite groups. They are in fact the only finite $t$-transitive permutation groups with $t > 3$ known other than the symmetric and alternating groups[25](p. 286).
Chapter 6

$M_{12}$ in Music

Having explored $M_{12}$ in some depth it is desirable to return to the origins of our motivation. This closing chapter examines how the French composer Oliviér Messiaen used the permutations of $M_{12}$ to compose his music. Specifically we will explore the 4th piece of his Quatre études de rythme (Four studies in rhythm) titled Île De Feu 2 (Island of Fire).

The earliest known example of mathematics appearing in musical composition comes from french mathematician and music theorist Marin Marsenne’s 1636 work Harmonie Universelle where he refers to arranging the order and distribution of notes via simple combinatorial mathematics\textsuperscript{22}(p. 936). It was in the early 20th century when the practice became more popular however. This time saw the revolution of atonal music which inspired the use of new musical scales which, unlike the conventional, featured equal length intervals between each note. Lacking the features of the classic musical scales useful in forming melody and structure, alternative methods for organising notes into a piece were needed. This opened the door for avant-garde approaches to harmonic organization - the symmetric nature of the scales allowing permutations to be employed in composition. Messiaen, Igor Stravinsky and Bela Bartók all composed using these innovative compositional notions - avoiding conventional harmonic structure and progression.
6.1 Île De Feu 2: A Breakdown

6.1.1 Pitch

Throughout his piece, Messiaen has been very kind to the musical analyst by marking the opening of any new melodic phrase with with a roman numeral (I to X). Each numeral represents a certain ordering of notes reached via a composition of the permutations $P_O$ and $P_I$ (which of course gives other permutations from $M_{12}$).

Returning to the system of assigning integers to the notes of the scale (discussed in Chapter I), note that that Messiaen’s assignment of numbers ($B$ in Figure 1.1) is not as random as it appears on first glance. The natural chromatic numbering of notes (marked $A$ in the Figure 1.1) when permuted once by $P_O$ and then numbered 1 to 12 from left to right in fact yields Messiaen’s choice.

Notes after numeral I in the upper voice in Messiaen’s piece (annotated onto the simplified excerpt in Appendix D) are $F^\# - F - G - E - G^\# - D^\# - A - D^\# - A - C - B - C$ which is simply 1 ascending to 12 in Messian’s allocation of numbers, i.e. the identity permutation on $B$. The next intervention marked on the script is III after which come the notes $C^\# - E - G - A^\# - B - G^\# - F - D - C - D^\# - F^\# - A$. Comparing to their corresponding integers we have 9-3-2-8-10-4-1-7-11-5-0-6. This is simply I permuted twice by $P_O$ however. In fact the notes after each roman numeral $N$ are given by $P_O^{N-1}(B) = P_O^N(A)$.

Looking now to the lower voice, after I we have notes $A - D^\# - D^\# - E - C^\# - G^\# - B - F - C - F^\#$ (again see Appendix D) which in integer notation is 7-6-8-5-9-4-10-3-11-2-12-1. This particular ordering of notes is obtained from permuting $B$ with $P_O$ once again. The note string Messiaen denotes with II is then a further permutation of I by $P_O$ and so on such that notes after numeral $N$ correspond to $P_O^N(B) = P_O^{N+1}(A)$.

6.1.2 Note Duration

Other musical parameters such as rhythm, tempo, dynamics and articulation are more difficult to organise into discrete units but Messiaen has rather impressively
used the same method - applied to 12 distinct units of time - to dictate his choice of note durations in the piece\footnote{p. 410}. The musical notation for 12 durations are given below in both sounded note form and rest form (instructing a certain interval of silence). Their lengths increase from left to right - their relative length to a whole note being written below. We number them with integers modulo 11 just as before.

![Figure 6.1: Note Durations](image)

Let us denote the numbering above $A_D$ since it is equivalent to $A$ in the previous section. The order of durations printed after numeral I is reached via permutation of this $A_D$ by $P_I$ this time. Very similarly to the treatment of note composition, durations seen after II in his piece correspond to a further $P_I$ permutation applied to I and so on such that numeral N dictates note durations in the order given by $P_N(A_D)$. It should be noted that 'rests' are included in this construction. That is, those periods of silence where no notes are sounded ‘count’ in the sequence of note durations.

### 6.2 Messiaen’s Charm of Impossibilities

The key role of $M_{12}$ in the construction of each section of the piece then is clear. It is however recommended that the reader look closely at the excerpt of Île De Feu 2 contained in the appendix and the music itself\footnote{21} to gain full appreciation of the process by personally verifying this system of composition. Clearly his short but energetic piece Île De Feu 2 features a diminutive subset of the 95,040 permutations in the group, but it was allowing the listener just a glimpse of what may occur when one continues in this way which he enjoyed and found
inspiration in. He believed that his innovative use of symmetrical permutations in his music amongst other concepts involving mathematical structure added a mystical dimension to his compositions. He called this phenomenon the ‘charm of impossibilities’ [7].

Composers with even the slightest knowledge of mathematics employ basic relations and patterns in many aspects of music. Indeed in 1712 Leibniz wrote: ‘Music is the pleasure the human mind experiences from counting without being aware that it is counting’ [22] (p. 935). Order and reason as well as pattern and transformation are central concepts in both disciplines. While music has derived inspiration from mathematics, mathematics provides the tools for creation (in groups like $M_{12}$) as well as a language for articulating musical analysis [22] (p. 943-944).
## Appendix A

### Cols and Tets

<table>
<thead>
<tr>
<th>+</th>
<th>+</th>
<th>+</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table A.1: Examples of *cols*

<table>
<thead>
<tr>
<th>+</th>
<th>+</th>
<th>+</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
<th>+</th>
<th>+</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>+</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
<th>+</th>
<th>+</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>0</td>
<td>-</td>
<td>+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
<th>+</th>
<th>+</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>+</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
<th>+</th>
<th>+</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>+</td>
<td>0</td>
</tr>
</tbody>
</table>

Table A.2: Examples of *tets*
Appendix B

Crosses and Squares

Table B.1: Crosses and Squares: Examples
Appendix C

Kitten in the Shuffle Labelling

\begin{center}
\begin{tabular}{|c|c|c|c|}
\hline
0 & 3 & \infty & 2 \\
5 & 9 & 8 & 10 \\
4 & 1 & 6 & 7 \\
\hline
\end{tabular}
\end{center}

Table C.1: MINIMOG in the Modulo 11 Labelling

\begin{center}
\begin{tabular}{cccccc}
6 & \\
9 & \\
10 & 8 & \\
7 & 2 & 5 & \\
9 & 4 & 11 & 9 & \\
10 & 8 & 3 & 10 & 8 & \\
\end{tabular}
\end{center}

Table C.2: Kitten in the *Shuffle Labelling*

\begin{center}
\begin{tabular}{ccc|ccc|ccc}
5 & 11 & 3 & 5 & 11 & 3 & 8 & 10 & 3 \\
8 & 2 & 4 & 2 & 4 & 8 & 9 & 11 & 4 \\
9 & 10 & 7 & 7 & 9 & 10 & 5 & 2 & 9 \\
6 & 1 & 0 & \\
\end{tabular}
\end{center}

Table C.3: Views from 3 points-at-\infty
Appendix D

Excerpt from *Île De Feu* 2
Bibliography


