The Mathieu Group M_{12} and Conway's M_{13}-Game

Senior Honors Thesis in Mathematics

Jeremy L. Martin

under the supervision of Professor Noam D. Elkies

Harvard University

April 1, 1996

Part I

Introduction

Although the Mathieu groups are probably best known today as the first instances of the sporadic simple groups, Mathieu's discovery of them arose rather from his search for highly transitive permutation groups; only later were the Mathieu groups shown to be simple. In modern mathematics, the Mathieu groups are studied chiefly in conjunction with sphere packing and error-correcting codes. Conway [3] has recently proposed an unusual method of constructing the Mathieu group M_{12}, which has a natural extension to a larger quasigroup, heretofore unknown, named by Conway "M_{13}". Conway's original article leaves the investigation of this construction as an open problem.

We begin from a classical point of view, describing the Mathieu groups in terms of their most salient properties, multiple transitivity and simplicity. With this material in the background, we move to a discussion of Conway's construction of the group M_{12} and the quasigroup M_{13}, as set forth in Conway's original article and a subsequent paper of Elkies [6]. In particular, we examine a metric on M_{13}, induced naturally by the Conway construction, and determine the extent to which M_{13} is sextuply transitive. Finally, we discuss an extension of the Conway construction, known to Conway and explored further by Elkies, inducing signed extensions $2M_{13}$ and $2M_{12}$.

This thesis consists in part of a summary of previous work on the Mathieu groups, and in part of original work by the author. In particular, the sections dealing with the metrization of M_{13}, sextuple transitivity, and antipodes in $2M_{13}$, culminating in Theorems IV.1, IV.4, IV.10, and IV.15, are my own research, carried out under the supervision of Professor Noam Elkies. This research was facilitated by a computer program that I designed to implement the Conway construction.

Thanks are due, first and foremost, to my advisor, Professor Noam D. Elkies, for his devoted attention to every aspect of this work. I would also like to acknowledge Professor M. Krishnamoorthy for providing me with Conway's seminal article on M_{13}, and finally Professor John H. Conway himself, without whose insight much of this thesis would not exist.

Part II

Multiply Transitive Groups

1 Introduction

A group G acting on a set S is said to be *k-transitive* if any k-tuple of distinct elements of S can be taken to any other k-tuple by an appropriate element of G. If that element is unique, G is *exactly k-transitive*. Mathieu's original discovery of the groups that bear his name grew out of his effort to construct highly transitive permutation groups. In fact, groups exhibiting greater than double transitivity are quite rare; it is known [5, 7] that no nontrivial sextuply transitive groups (i.e., highly transitive groups other than S_n and A_n) exist, and furthermore that M_{12} and M_{24} are the only nontrivial quintuply transitive groups.

2 Construction of Highly Transitive Groups

Greenberg [5, pp. 13–15] describes an elementary method, developed by Witt and others, for constructing multiply transitive permutation groups. In order to best understand this method, we follow Greenberg's presentation of first examining how such highly transitive groups are built up internally.

Let $G = G^{(t)}$ act t-transitively on a set $X_t = \{p_1, \ldots, p_r,\ q_1, \ldots, q_t\}$ and define $G^{(i)}$ to be the stabilizer of the points $\{q_{i+1}, \ldots, q_t\}$ in G. The group $G^{(i)}$ can be characterized equivalently as the action of G restricted to $X_i = \{p_1, \ldots, p_r,\ q_1, \ldots, q_i\}$, or as the stabilizer of q_i in $G^{(i+1)}$, for $i < t$. This last description implies that $G^{(i)}$ is a proper subgroup of $G^{(i+1)}$, because $G^{(i+1)}$ does not fix q_i but $G^{(i)}$ does. Thus there is a strictly decreasing chain of subgroups

$$G = G^{(t)} \ > \ G^{(t-1)} \ > \ \cdots \ > \ G^{(1)} \ > \ G^{(0)} = H$$

where $G^{(i)}$ acts i-transitively on X_i for $i = 1, \ldots, t$.

Now, for all $i \geq 2$, we can find an element s_i of $G^{(i)}$ which interchanges q_{i-1} with q_i and fixes q_j for $j < i-1$. (Such an s_i must exist, since $G^{(i)}$ is i-transitive.) We can write $s_i = a_i t_i = t_i a_i$, where t_i is the involution $(q_{i-1}\ q_i)$ and $a_i \in H$.

Proposition II.1: Given s_i and $G^{(i)}$ as above, the following properties hold:

1. $s_i^{-1} H s_i = H \qquad (i \geq 2)$;
2. $s_i^{-1} G^{(1)} s_i = H \qquad (i \geq 3)$;
3. $(s_i s_j)^{m_{ij}} \in H$, where $m_{ij} = \begin{cases} 1: & i = j \\ 3: & |i-j| = 1 \\ 2: & |i-j| > 1 \end{cases}$;
4. $G^{(i)} = G^{(i-1)} \ \cup \ G^{(i-1)} s_i G^{(i-1)}$.

Only (4) requires any detailed proof. Since $G^{(i-1)} < G^{(i)}$ and $s_i \in G^{(i)}$ by definition, $G^{(i)}$ contains $G^{(i-1)} \cup G^{(i-1)} s_i G^{(i-1)}$. Moreover, any permutation of $G^{(i)}$ which fixes q_i lies in $G^{(i-1)}$. On the other hand, if some element $\sigma \in G^{(i)}$ does not fix q_i, then we must find $\alpha, \beta \in G^{(i-1)}$ such that $\sigma = \alpha s_i \beta$. In fact, it suffices to produce α, β such that $\sigma \cong \alpha s_i \beta \bmod H$ (i.e., σ and $\tau = \alpha s_i \beta$ act identically on all q_j). This follows since $h = \tau^{-1}\sigma$ fixes all q_j and so lies in $H < G^{(i-1)}$, whence $\sigma = \tau h = \alpha s_i (\beta h)$, and $\beta h \in G^{(i-1)}$.

Choose some $\alpha \in G^{(i-1)}$ taking q_{i-1} to $\sigma(q_i)$, and let $c_j = \alpha^{-1}(\sigma(q_j))$. Then choose $\beta \in G^{i-1}$ such that $\beta(q_j) = s_i^{-1}(c_j)$ for all $j < i$. Therefore:

$$\alpha(s_i(\beta(q_i))) = \alpha(s_i(q_i)) = \alpha(q_{i-1}) = \sigma(q_i)$$

and

$$\alpha(s_i(\beta(q_j))) = \alpha(c_j) = \sigma(q_j) \qquad (j < i)$$

Hence $\alpha s_i \beta$ and σ act identically on the q_j, and we are done. □

From this elementary analysis, it is apparent how the construction of multiply transitive groups will proceed. We begin with a group $G^{(1)}$ acting transitively on a set $X_1 = \{p_1, \ldots, p_r,\ q_1\}$, with a subgroup $H = \mathrm{Stab}_{q_1} G^{(1)}$. We

then successively adjoin elements $q_2, \ldots, q_t$ to X_1 and permutations $s_2, \ldots, s_t$ to $G^{(1)}$ satisfying the conditions of Proposition II.1, producing a chain of groups

$$H \ < \ G^{(1)} \ < \ \cdots \ < \ G^{(i)} = G^{(i-1)} \ \cup \ G^{(i-1)} s_i G^{(i-1)} \ < \ \cdots \ < \ G^{(t)},$$

where $G^{(i)}$ acts i-transitively on $\{p_1, \ldots, p_r, \ q_1, \ldots, q_i\}$.

To make this procedure explicit, let $G^{(i)}$ be a group acting i-transitively on $X_i = \{p_1, \ldots, p_r, \ q_1, \ldots, q_i\}$. Adjoin a new element q_{i+1} to form $X_{i+1} = X_i \ \cup \ \{q_{i+1}\}$. Let s_{i+1} be a permutation which interchanges q_i with q_{i+1} and fixes q_j for $j < i$. That is, $s_{i+1} = a_{i+1} t_{i+1}$, where t_{i+1} is the involution $(q_{i+1} \ q_i)$ and $a_{i+1} \in H$.

Theorem II.2 (Greenberg): The set $G^{(i+1)} = G^{(i)} \ \cup \ G^{(i)} s_{i+1} G^{(i)}$ acts $(i+1)$-transitively on X_{i+1}.

Proof: It is sufficient to show that any i-tuple $(x_1, \ldots, x_{i+1})$ in X_{i+1} can be transformed to $(q_1, \ldots, q_{i+1})$ by an appropriate permutation $\sigma \in G^{(i+1)}$. If $x_{i+1} = q_{i+1}$, then the desired σ can be found in $G^{(i)}$. Otherwise, choose $\beta \in G^{(i)}$ taking x_{i+1} to q_i, and choose $\alpha \in G^{(i)}$ taking $s_{i+1}(\beta(x_j))$ to q_j for $j < i$. Since $\alpha(s_{i+1}(\beta(x_{i+1}))) = \alpha(s_{i+1}(q_i)) = \alpha(q_{i+1}) = q_{i+1}$, the permutation $\alpha s_{i+1} \beta$ is the desired element of $G^{(i)} s_{i+1} G^{(i)}$. $\square$

The limitation of this method is that the set $G^{(i+1)}$ need not be a group. Certainly $G^{(i)}$ is closed under multiplication, and $G^{(i)} s_{i+1} G^{(i)}$ is closed under both left and right multiplication by $G^{(i)}$, but there is no guarantee, in general, that the product of two elements of $G^{(i)} s_{i+1} G^{(i)}$ must lie in $G^{(i+1)}$. However, Witt showed the following result (discussed without proof in [5, p. 15]; the theorem is stated slightly differently in [7, pp. 220–1], which facilitates the construction of transitive extensions:

Theorem II.3 (Witt): Let a group $G^{(2)} = G^{(1)} \ \cup \ G^{(1)} s_2 G^{(1)}$ act doubly transitively on $\{p_1, \ldots, p_r, \ q_1, \ q_2\}$, where $G^{(1)} = \mathrm{Stab}_{q_2} G^{(2)}$. Choose extension elements $\{s_2, \ldots, s_n\}$ satisfying the conditions of Proposition II.1. Then $G^{(i+1)}$, defined recursively as $G^{(i)} \ \cup \ G^{(i)} s_{i+1} G^{(i)}$, is a group.

Hence, if we can find the right permutations to adjoin to create the chain $G^{(1)} \ < \ \cdots \ < \ G^{(t)}$, Theorem II.3 ensures that $G^{(i+1)} = G^{(i)} \cup G^{(i)} s_{i+1} G^{(i)}$

is "small." (Recall that we are trying to construct a transitive group other than a symmetric or alternating group.) We can compute the order of $G^{(i+1)}$ easily: since $G^{(i)} = \mathrm{Stab}_{q_{i+1}} G^{(i+1)}$, the index $[G^{(i+1)} : G^{(i)}]$ equals $r+i$, the number of points permuted by $G^{(i+1)}$. Hence $|G^{(i+1)}| = (r+i) \cdot |G^{(i)}|$.

3 Constructions of the Mathieu Groups

The following constructions of the Mathieu groups, borrowed directly from [5, pp. 15–21], proceed according to the method described above, thus confirming the groups' multiple transitivity. Since repeatedly checking that Proposition II.1 is satisfied for each step in the chain would be tedious, we omit these verifications (which are provided by Greenberg), giving simply the initial groups and extension elements at each stage. (Conway and Sloane [4, pp. 273,274] give generators and relations for the Mathieu groups, as well as different constructions which are more pertinent to the Mathieu groups' role as groups of automorphisms of the Golay codes, and prove the quintuple transitivity of M_{12} and M_{24} by other means.)

3.1 Constructing M_{10}, M_{11} and M_{12}

Let F_9 denote the field of nine elements, whose group of units is $F_9^* = F_9 \setminus \{0\}$. Let α be a primitive element in F_9 (i.e., one generating the cyclic group of units). Note that $\alpha + \alpha^2 = 1$, facilitating arithmetic in F_9 [5, p. 16]. For $a \in F_9^*$, define γa to be 1 if a is a square, 3 otherwise. Since the eighth power of any element of F_9^* is 1, the map γ is a homomorphism from F_9^* to the multiplicative group $(\mathbf{Z}/8\mathbf{Z})^*$.

For $a \in F_9^*$, let $\sigma_{a,0} : F_9 \to F_9$ be the map taking x to $ax^{\gamma a}$. The set of all such maps is a group, because $\sigma_{a,0}(\sigma_{b,0}(x)) = a(bx^{\gamma a})^{\gamma b} = (ab)x^{(\gamma(ab)} = \sigma_{ab,0}(x)$ (using the fact that the eighth power of any element in F_9^* is 1). Moreover, it is transitive on F_9^* because $\sigma_{a,0}(1) = a$. This set of maps will be our group $G^{(1)}$. Since every map in $G^{(1)}$ fixes 0, we will let $q_1 = 0$ and $p_1, \ldots, p_8$ be the nonzero elements of F_9. Note that the stabilizer of any p_i, i.e., the group H, is trivial.

The next link in our chain is the group $G^{(2)}$, consisting of all maps $\sigma_{a,b}$

taking x to $ax^{\gamma a} + b$, where $a \in F_9^*$, $b \in F_9$. Using the terminology of Theorem II.2, $G^{(2)}$ is obtained by adjoining to $G^{(1)}$ the involution $s_2 = \sigma_{-1,1}$, which interchanges x with $1 - x$. The group $G^{(2)}$ has order 72 (since there are 8 choices for a and 9 choices for b) and is doubly transitive, since for any $c, d \in F_9$, $c \neq d$, the map $\sigma_{c-d,d}$ takes 1 to c and 0 to d.

To obtain the groups $G^{(3)}$, $G^{(4)}$, and $G^{(5)}$, we adjoin points $q_3 = \infty$, $q_4 = V$, and $q_5 = W$ to F_9 (the naming of the points is Greenberg's), and the permutations s_3,s_4,s_5 described below. (Note that the conditions of Proposition II.1 are satisfied.)

$$s_3 \ : \ x \mapsto x^{-1};$$
$$s_4 \ : \ x \mapsto \alpha^2 x + \alpha x^3 \ (x \in F_9), \qquad V \longleftrightarrow \infty;$$
$$s_5 \ : \ x \mapsto x^3, \qquad V \longleftrightarrow W.$$

The following groups are produced. (Note that the group $M_{10} = G^{(3)}$, unlike the other Mathieu groups, is not simple; it has a subgroup of index 2 which is isomorphic to the alternating group A_6 [4, p.272].)

$M_{10} = G^{(3)}$:	3-transitive on $F_9 \cup \{\infty\}$,	order $10 \cdot \lvert G^2 \rvert = 720$;
$M_{11} = G^{(4)}$:	4-transitive on $F_9 \cup \{\infty, V\}$,	order $11 \cdot \lvert G^3 \rvert = 7920$;
$M_{12} = G^{(5)}$:	5-transitive on $F_9 \cup \{\infty, V, W\}$,	order $12 \cdot \lvert G^4 \rvert = 95040$.

3.2 Constructing M_{22}, M_{23} and M_{24}

Let F_4 denote the field of four elements, with a primitive element ρ. Let P_4 denote the projective plane of order four, which can be realized as $F_4^3 \setminus \{(0,0,0)\}$ modulo the relation $x = kx$. We will refer to the elements of P_4 by any of the points of their lifts in $F_4^3 \setminus \{0,0,0\}$.

Our doubly transitive group $G^{(2)}$ will be the projective special linear group $PSL_3(F_4)$, which is the quotient of the special linear group $SL_3(F_4)$ by its center Z consisting of all maps $x \mapsto kx$, $k \in F_4 \setminus \{0\}$. Since there are three choices for k and the cube of any nonzero element of F_4 is 1, the group Z is cyclic of order three. To compute $|G^{(2)}|$, first note that $|\, GL_3(F_4)| = (4^3-1)(4^3-4^1)(4^3-4^2) = 181440$ [7, p. 162]. Since $[GL_3(F_4) : SL_3(F_4)] = 3$ and $[SL_3(F_4) : Z] = 3$, we obtain $|G^{(2)}| = |\, PSL_3(F_4)| = 181440/3^2 =$

20160. Moreover, $G^{(2)}$ is doubly transitive on P_4 because $SL_3(F_4)$ is doubly transitive on F_4^3, and the quotient map from $SL_3(F_4)$ to $PSL_3(F_4)$ is the same as that from F_4^3 to P_3.

Let $q_2 = (1,0,0)$ and $q_1 = (0,1,0)$. The group $G^{(1)} = \mathrm{Stab}_{q_2} G^{(2)}$ may be presented as the set of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & c & d \\ 0 & e & f \end{pmatrix}$$

where $a, b, c, d, e, f \in F_4$ and $cf - de = 1$. Then $G^{(0)} = \mathrm{Stab}_{q_1,q_2} G^{(2)}$ is the set of matrices in the above form where $a = e = 0$ (and thus $cf = 1$).

To obtain the groups $G^{(3)}$, $G^{(4)}$, and $G^{(5)}$, we add points q_3, q_4, q_5 to P_4, and adjoin the following permutations s_3, s_4, s_5 to $G^{(2)}$. (Note that, as required, we have s_i fixing q_j whenever $j \leq i - 2$.)

$$s_3 : (x,y,z) \mapsto (x^2 + yz, y^2, z^2) \qquad ((x,y,z) \neq (1,0,0)), \qquad q_2 \longleftrightarrow q_3;$$

$$s_4 : (x,y,z) \mapsto (x^2, y^2, \rho z^2), \qquad q_3 \longleftrightarrow q_4;$$

$$s_5 : (x,y,z) \mapsto (x^2, y^2, z^2), \qquad q_4 \longleftrightarrow q_5.$$

Once again, the conditions of Proposition II.1 hold at each step, and the resulting groups are as follows:

$$\begin{array}{lll} M_{22} = G^{(3)}: & \text{3-transitive on } P_4 \cup \{q_3\}, & \text{order } 22 \cdot |G^2| = 443520; \\ M_{23} = G^{(4)}: & \text{4-transitive on } P_4 \cup \{q_3, q_4\}, & \text{order } 23 \cdot |G^3| = 10900960; \\ M_{24} = G^{(5)}: & \text{5-transitive on } P_4 \cup \{q_3, q_4, q_5\}, & \text{order } 24 \cdot |G^4| = 244823040. \end{array}$$

4 The Simplicity of the Mathieu Groups

Rotman [7, p. 226] proves that the Mathieu groups are simple. We omit the proof, since it rests on a substantial amount of nonelementary group theory and will not be used in subsequent sections. A more elementary proof of

the simplicity of M_{11} and M_{23} is given by Chapman [2], who further notes that the proof extends to M_{12} and M_{24} via a preliminary result also used in Rotman's proof.

Part III

The Golay Codes and the Mathieu Groups

1 Introduction

The Golay codes are two error-correcting codes of length 12 and 24, of substantial importance in coding theory and sphere packing. The Mathieu groups appear in the study of the automorphism groups of the Golay codes. The following discussion of the relationship between the Golay code C_{12} of length 12 and the Mathieu group M_{12} is largely due to chapter 10 in Conway and Sloane [4]. A roughly analogous relationship, which we shall not explore, holds between the Golay code C_{24} and the Mathieu group M_{24}.

2 The Golay Code C_{12}

Let Ω denote the projective line of order eleven, realized as $F_{11} \cup \{\infty\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, \infty\}$. (We borrow the computer scientist's convention of using the single letters A, B, C to denote the numbers 10, 11, 12.) We distinguish the following important subsets of Ω:

$$\Omega' = F_{11} = \Omega \setminus \{\infty\}; \qquad Q = \{x^2 \ : \ x \in F_{11}\} = \{0, 1, 3, 4, 5, 9\};$$
$$Q' = Q \setminus \{0\} = \{1, 3, 4, 5, 9\}; \qquad N = \Omega \setminus Q = \{2, 6, 7, 8, A, \infty\}.$$

(The names Q and N refer to the quadratic residues and nonresidues, respectively, modulo 11.) Arithmetic in Ω is an extension of that in F_{11}, with

the additional provisions that $\infty + a = \infty$ for any $a \in \Omega$ (including ∞ itself), $a/0 = \infty$ for $a \in \Omega \setminus \{0\}$, and $a/\infty = 0$ for $a \in \Omega'$.

Now let X be a 12-dimensional vector space over F_3, equipped with a basis $\{x_i\}$ indexed by $i \in \Omega$. Define

$$w_\infty = \sum_{i \in \Omega} x_i$$

and

$$w_i = \left(\sum_{n \in N} x_{n-j} \right) - \left(\sum_{q \in Q} x_{q-j} \right), \qquad i \in \Omega'.$$

The *Golay code* C_{12} consists of the vectors in the space spanned by $\{w_i\}$ for $i \in \Omega$. A complete investigation of the properties of C_{12} is beyond the scope of this paper. We will prove herein merely that the code has dimension 6 and is self-dual, as a preamble to our discussion of the relationship between C_{12} and M_{12}. In fact, the Golay code is the only code of minimal distance greater than 3 satisfying these conditions [4, p. 434].

The following definition will be useful. Let $w_{i,j}$ denote the projection of w_i onto the vector space spanned by x_j. By the definition of the vectors w_i,

$$w_{i,j} = \begin{cases} 1 & : i + j \in N \\ -1 & : i + j \in Q \end{cases}$$

Conveniently, $w_{i,j}$ depends only on the sum $i + j$. In particular, $w_{i,j} = w_{j,i}$, which is the first suggestion of the self-duality of C_{12}. The next theorem, although we use it simply as a stepping-stone in the proof that $\dim(C_{12}) = 6$, illuminates some of the structure of C_{12} as an error-correcting code.

Lemma III.1: Any number $z \in F_{11} \setminus \{0\}$ can be written exactly three ways as $q - q'$ and exactly two ways as $n - n'$, where $q, q' \in Q$ and $n, n' \in N$.

Proof: By inspection; simply write out all such differences $q - q'$ and $n - n'$. (Those familiar with design theory will recall that if p is a prime congruent

to 3 modulo 4, then the set of quadratic residues modulo p constitutes a difference set in F_p, which implies the Lemma.)

At this point, we introduce one more notational convenience: "$x \sim y$" will mean that x and y have the same quadratic character, i.e., either they both lie in Q or both lie in N.

Theorem III.2: For any distinct $j, k \in \Omega$, w_j and w_k agree in exactly six places. (I.e., $w_{j,i} = w_{k,i}$ for exactly six values of $i \in \Omega$.)

Proof: If $j = \infty$, then $w_{\infty,i} = 1$ for all i, but $w_{j,i} = 1$ exactly six times when $j \in \Omega$. Moreover, since $w_{i,j} = w_{i+j,0}$, it suffices to prove the statement of the theorem in the case where $j = 0$ and $k \in \Omega \setminus \{0\}$. Note that $w_{0,a} = w_{0,b} \Longleftrightarrow a \sim b$.

By Lemma III.1, there exist points $\{x_1, \ldots, x_5\}$ and $\{y_1, \ldots, y_5\}$ of Ω' such that $x_n \sim y_n$ and $x_n - y_n = k$ for $n = 1 \ldots 5$. We claim that $w_{k,i} = w_{0,i} \Longleftrightarrow i$ is either ∞ or one of the y_n.

"$\Rightarrow$": $w_{0,i} = w_{k,i} = w_{0,k+i}$, so $i \sim (k + i)$. If $i \neq \infty$, then $(k + i, i)$ must be one of the (x_n, y_n).

"$\Leftarrow$": Clear when $i = \infty$. If $i = y_n$, then $w_{k,y_i} = w_{0,k+y_i} = w_{0,x_i} = w_{0,y_i}$ (since $x_i \sim y_i$).

Hence the theorem is proven. □

Corollary III.3: For any $j, k \in \Omega$,

$$\sum_{i \in \Omega} (w_{i,j} w_{i,k}) = 0.$$

Proof: If $j = k$, then the sum is $12 = 0$ (since we are working in F_3). If $j \neq k$, the sum is $6(1) + 6(-1) = 0$. □

We next prove that $\dim(C_{12}) = 6$. That the dimension is no greater than 6 follows from Corollary III.3, which by bilinearity implies that the scalar product of any two vectors in W is zero. This in turn implies that W is contained inside its dual space $W^{\perp}$, so $\dim(W) \leq \dim(W^{\perp})$. Since $\dim(W) + \dim(W^{\perp}) = 12$, it follows that $\dim(W) \leq 6$.

To prove that $\dim(C_{12})$ is exactly 6, we show that the six vectors $\{w_i\}$, $i \in (Q \cup \{\infty\})$, are linearly independent. We use the fact that if $W' \subset W$ is a linear space spanned by vectors $S \subset \{w_i\}$, and there exists a pair $j, k \in \Omega$ such that $w_{i,j}$ is a multiple of $w_{i,k}$ for all $w_i \in S$, then the same property holds for any vector of W' by linearity. Conversely, any w_i not satisfying this property does not lie in W'. In this fashion, using $(j,k) = (5,9),\ (4,5),\ (3,9),\ (1,3),\ (1,4)$, we learn respectively that each of $w_1,\ w_3,\ w_4,\ w_5,\ w_9$ does not lie in the space spanned by the other four. Hence these five vectors are linearly independent. Suppose w_∞ lies in this space. Then we have a linear relation

$$w_\infty = \sum_{i \in Q'} c_i w_i \qquad (c_i \in F_3).$$

Now, $w_{\infty,i} = 1$ for all i. Therefore, for any pair j, k, the sum of all c_i such that $w_{i,j} = -w_{i,k}$ must be 0. Fixing $j = \infty$ and letting k equal $1, 3, 4, 5, 9$, we learn respectively that $c_3 + c_4,\ c_1 + c_9,\ c_1 + c_5,\ c_4 + c_9,\ c_3 + c_5$ are all zero. Thus each individual c_i can only be zero, and hence w_∞ is linearly independent as desired. □

Having gained some familiarity with the structure of C_{12}, let us examine its group of automorphisms. Define linear operators A, B, C, D on X as follows:

$$\begin{aligned} A &: x_i \mapsto x_{i+1}, \\ B &: x_i \mapsto x_{3i}, \\ C &: x_i \mapsto \varepsilon x_{-1/i}, \\ D &: x_i \mapsto x_{\delta i}, \end{aligned}$$

where $\varepsilon = 1$ for $x \in Q$ and -1 for $x \in N$, and δ is the permutation $(2\ A)(3\ 4)(5\ 9)(6\ 7)$.

It can be verified that A, B, C, D preserve C_{12}. Specifically,

$$\begin{aligned} A &: w_i \mapsto w_{i-1}, \\ B &: w_i \mapsto w_{3i}, \\ C &: w_i \mapsto -\varepsilon w_{-1/i}, \\ D &: w_i \mapsto w_{\delta i}. \end{aligned}$$

Hence the group $G = \langle A, B, C, D \rangle$ is a subgroup of the automorphism group of C_{12}. (In fact, G contains every automorphism of C_{12}; this is stated but not proven in [4].) G is a group $2M_{12}$, i.e., it has a normal subgroup N, cyclic of order 2, and the quotient group G/N is isomorphic to M_{12}. (The involution generating N is the permutation C^2, which takes every basis vector x_i to its negative.) However, G is a "non-splitting extension" of M_{12}, i.e., it does not have a subgroup isomorphic to M_{12} [4, pp. 271–2].

3 Steiner Systems

A *Steiner system* $S(t, k, v)$ is defined as a set of v points, organized into $\binom{v}{t}/\binom{k}{t}$ blocks of k points each, such that any subset of t points is contained in exactly one of the blocks [5, 7]. The projective plane of order n, for instance, is a Steiner system $S(n^2 + n + 1, n + 1, 2)$. Note that a Steiner system need not exist for every choice of parameters t, k, v; in particular $\binom{v}{t}/\binom{k}{t}$ must be an integer. An open problem in design theory is to determine necessary and sufficient relations among the parameters for $S(t, k, v)$ to exist, as well as to determine how many Steiner systems exist, up to isomorphism, for each values of v, k, and t.

The Mathieu groups can be realized as automorphism groups of certain Steiner systems [4, 5]. (An automorphism of a Steiner system is a permutation of the v points which carries every block to a block.) In particular, the supports of the codewords of C_{12} constitute a Steiner system $S(5, 6, 12)$, of which M_{12} is the automorphism group. The stabilizer of one point, the group M_{11}, is the automorphism group of a Steiner system S(4,5,11). Analogously, the group M_{24} is the automorphism group of a Steiner system $S(5, 8, 24)$ obtained by taking the supports of the codewords of the Golay code C_{24}, and M_{23} and M_{22}, the stabilizers of one and two points respectively, are the automorphism groups of $S(4, 7, 23)$ and $S(3, 6, 22)$. Although we are primarily concerned herein with examining the Mathieu groups as automorphism groups of the Golay codes, their role as automorphisms of Steiner systems is also important in design theory.

Part IV

The Conway Game and M_{13}

1 Introduction

Let P_3 denote the projective plane of order 3. The standard construction of P_3 is to remove the zero point from a three-dimensional vector space over the field F_3 and then identify each point x with $-x$, obtaining a space with $(3^3 - 1)/2 = 13$ points. However, we will be concerned only with the geometric properties of the projective plane. The 13 points of P_3 are organized into 13 lines, each line containing four points. Every point lies on four lines, any two points lie together on a unique line, and any two lines intersect at a unique point. We shall borrow the following numbering of the lines and points of P_3 from Conway's article. (Note that the numbering is self-dual, in the sense that point i lies on line j iff point j lies on line i.)

Line	Points	Line	Points
0	$0, 1, 2, 3$	7	$3, 5, 8, B$
1	$0, 4, 5, 6$	8	$3, 4, 7, A$
2	$0, 9, A, B$	9	$2, 4, B, C$
3	$0, 7, 8, C$	A	$2, 6, 8, A$
4	$1, 4, 8, 9$	B	$2, 5, 7, 9$
5	$1, 6, 7, B$	C	$3, 6, 9, C$
6	$1, 5, A, C$		

Conway [3] proposed the following game, which resembles Sam Loyd's well-known "15-puzzle." Place twelve numbered counters on the points $0 \ldots B$ of P_3 and leave the thirteenth point C blank. (The empty point will be referred to throughout as the "hole.") Let the location of the hole be p; then a *primitive move* of the game consists of selecting one of the lines containing the hole, say $\{p, q, r, s\}$. Move the counter on q to p (thus moving the hole to q), then interchange the counters on r and s. Following Elkies [6], we will use the notation ι_{pq} to refer to this particular primitive move. A *move* is any sequence $\iota_{ab}\iota_{bc} \ldots \iota_{xy}\iota_{yz}$ of primitive moves. For brevity, we will refer to a move by its *path* $abc \ldots xyz$ (specifically, the path that the hole

traces through P_3) and say that that path *produces* the move $\iota_{ab}\iota_{bc}\ldots\iota_{xy}\iota_{yz}$. Finally, the *length* of a move is the number of its constituent primitive moves, i.e., $|\{\iota_{ab},\ \ldots,\ \iota_{yz}\}|$.

There is an obvious characterization of a move as a permutation in S_{13}, operating on the points of P_3. By limiting our consideration to only those moves which return the hole to its starting point (i.e., those produced by a path $abc\ldots xyz$ with $a = z = C$), we obtain the *Conway game group*. This group, which we shall denote by G_C, is a subgroup of the symmetric group S_{12} of permutations of the twelve points $0, \ldots, B$, and the group operation of G_C is concatenation of paths. Conway [3] stated, but did not prove explicitly, that G_C is isomorphic to the Mathieu group M_{12}. We shall subsequently verify this isomorphism.

The set of all moves (including those not fixing the hole) is given the name M_{13} by Conway. It is important that M_{13} is not a group, as not all concatenations are legal: for two paths $P = x_1 \ldots x_a$ and $P' = y_1 \ldots y_b$, the path PP' is well-defined only if $x_a = y_1$. (This difficulty does not arise in G_C, where $x_1 = x_a = y_1 = y_b = C$.) M_{13} can nevertheless be thought of as a "quasigroup" permuting the thirteen points of P_3. Indeed, M_{13} exhibits certain limited forms of sextuple transitivity, which we shall later explore more fully.

Elkies [6] investigated an extension of the Conway game (known to Conway) in which the counters r and s are flipped upside down as well as interchanged. In this "signed Conway game", the set of all closed paths is a subgroup of $2M_{12}$, and the set of all paths is a quasigroup $2M_{13}$, which bears a similar relation to M_{13} as $2M_{12}$ does to M_{12}. One consequence hereof is that G_C is a subgroup of M_{12}. Although this constitutes half of the verification of Conway's claim, we defer presenting the particulars of Elkies' argument until later, since the inclusion result is inextricable from the main thrust of his work, which was to investigate the extension of M_{12} and M_{13} to their double covers $2M_{12}$ and $2M_{13}$.

2 The Computer Construction of M_{12} and M_{13}

I have written a computer program "MAKE–M13" (reproduced in the Appendix) to generate moves of the Conway game and compute the element of

M_{13} produced by each. The algorithm is simple. A list L of permutations in M_{13}, and paths that produce them, is maintained throughout execution. Paths are examined in increasing order of length; paths of the same length are examined in dictionary order (using $0 < 1 < \cdots < 9 < A < B < C$.) For each path P, the program first computes the permutation x produced by P, then checks to see if $x \in L$. If so, P is ignored and the next path examined; otherwise, P and x are placed in L, and the count of elements is incremented. Thus we are guaranteed to find a path of minimal length for each permutation in M_{13}. The algorithm was terminated when $1235520 = |M_{13}|$ elements had been found, as Elkies' results proved that there could be no more.

That MAKE–M13 was able to generate $|M_{12}| = 95040$ distinct permutations fixing the hole completes the verification that $M_{12} = G_C$. Rather than list all 95040 elements of the group here, I give two constructions of M_{12}, using particular elements found by MAKE–M13. Both imply that $M_{12} < G_C$, which, combined with Elkies' proof of the reverse inclusion, verifies Conway's assertion.

1. **The generators argument.** Conway describes M_{12} as a subgroup of the symmetric group S_{12} acting on the points $0, \ldots, 9, X, \infty$ [4, p. 273] and gives generators for M_{12} as follows:

$$\begin{aligned} \alpha &= (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ X)(\infty), \\ \gamma &= (0\ \infty)(1\ X)(2\ 5)(3\ 7)(4\ 8)(6\ 9), \\ \delta &= (0)(1)(2\ X)(3\ 4)(5\ 9)(6\ 7)(8)(\infty). \end{aligned}$$

Let Conway's $0, \ldots, 9, X, \infty$ correspond to points $1, 6, 9, A, B, 5, 8, 4, 2, 7, 3, 0$ of P_3. The following moves of the Conway game induce permutations corresponding to α, γ and δ respectively. (Here and subsequently, I use the paths found by MAKE–M13, which do not purport to be unique.)

Path	Permutation
$CB7485C$	$(1\ 6\ 9\ A\ B\ 5\ 8\ 4\ 2\ 7\ 3)(0)$
$C014C589C$	$(0\ 1)(3\ 6)(5\ 9)(4\ A)(2\ B)(7\ 8)$
$C357A2C$	$(0)(1)(2)(6)(3\ 9)(4\ 8)(5\ 7)(A\ B)$

2. **The quintuple transitivity argument.** We can construct M_{12} from elements of G_C by mimicking the construction given in II.3.1. We make the following correspondence between the points of $F_9 \cup \{\infty, V, W\}$ and the points of P_3 (recall that α denotes a primitive element of F_9):

$F_9 \cup \{\infty, V, W\}$:	1	α	α^2	α^3	α^4	α^5	α^6	α^7	0	∞	V	W
P_3:	0	1	2	4	7	6	5	3	9	8	A	B

The group $H = G^{(0)}$ is trivial, since M_{12} is exactly quintuply transitive. The group $G^{(1)}$ has eight elements and acts exactly 1-transitively on the set $\{0, \ldots, 7\}$. The nonidentity elements of $G^{(1)}$ are listed below; the names chosen for the elements of $G^{(1)}$ emphasize its isomorphism to a quaternion group. The first column denotes the value of a for which the permutation corresponds to the map $x \mapsto ax^{\gamma a}$ of II.3.1.

a	Name	Path	Permutation
α	i	$C106379C$	(0 1 7 6)(2 3 5 4)
α^2	j	$C20517AC$	(0 2 7 5)(1 4 6 3)
α^3	k	$C27B403C$	(0 4 7 3)(1 5 6 2)
α^4	-1	$C92059C$	(0 7)(1 6)(2 5)(3 4)
α^5	$-i$	$C379601C$	(0 6 7 1)(2 4 5 3)
α^6	$-j$	$C17A502C$	(0 5 7 2)(1 3 6 4)
α^7	$-k$	$C30427BC$	(0 3 7 4)(1 2 6 5)

To extend $G^{(1)}$ to the groups $G^{(2)}, \ldots, G^{(5)} = M_{12}$, it suffices to exhibit elements of G_C corresponding to the $s_2, \ldots, s_5$ of section II.3.1. These permutations are as follows:

Name	Path	Permutation
s_2	$C306C$	(0 9)(1 2)(3 6)(4 5)(7)(8)(A)(B)
s_3	$C0250C$	(0)(1 3)(2 5)(4 6)(7)(8 9)(B)(C)
s_4	$C0340C$	(0)(1 2)(3 4)(5 6)(7)(8 A)(9)(B)
s_5	$C09789C$	(0)(1 4)(2 5)(3 6)(7)(8)(9)(A B)

3 Metrizing M_{13} Via The Conway Game

Define the *depth* $D(x)$ of a permutation $x \in M_{13}$ to be the length of the shortest move of the Conway game which produces x. This definition arises naturally from the algorithm used to construct G_C — examine each path, in increasing order of length, and retain only the shortest path producing any permutation. A natural question to ask about the Conway game construction is: What are the *diameters* of $G_C = M_{12}$ and M_{13}, i.e., the maximal depth of any element? Additionally, which elements of M_{12} and M_{13} are the "deepest"?

The first step towards answering this and similar questions is to note that the Conway game provides us with a metric on M_{13}. Let x, y be two elements in M_{13}, produced by paths $x_1 \dots x_s$ and $y_1 \dots y_t$ respectively, where $x_1 = y_1 = C$. We would like to define the distance between a and b as the length of the shortest path from a to b. This can be realized as $d(x, y) = D(x^{-1}y)$. Note that the path of $x^{-1}y$ need not start at point C, so it may be necessary to relabel the points of P_3 to find an element equivalent to $x^{-1}y$. Also note that the depth of an element is simply its distance from the starting position, represented by the identity permutation.

It is easy to check that (M_{13}, d) satisfies the axioms of a metric space:

1. $d(x, y) = 0 \iff x^{-1}y = 1 \iff x = y$;
2. (Symmetry) $d(x, y) = d(y, x)$, because if a path P induces $x^{-1}y$, then the reversal of P induces $(x^{-1}y)^{-1} = y^{-1}x$;
3. (Triangle inequality) If $d(x, y) = a$ and $d(y, z) = b$, then by definition there exist paths P and Q of lengths a and b and producing $x^{-1}y$ and $y^{-1}z$ respectively. Then the concatenation PQ has length $a + b$ and produces the permutation $x^{-1}yy^{-1}z = x^{-1}z$. Having exhibited a path (albeit not necessarily the shortest) of length $a + b$ producing $x^{-1}z$, it follows that $d(x, z) \leq a + b = d(x, y) + d(y, z)$.

The first question posed, to find the diameters of M_{12} and M_{13}, can be answered empirically via MAKE–M13. In fact, we can state the number of elements of M_{12} and M_{13} at every depth, based on the MAKE–M13

construction; we have found no independent way to obtain results about the distribution.

Theorem IV.1: The depth distributions of M_{12} and M_{13} are as follows:

Depth	Permutations in M_{12}	Permutations in M_{13}
0	1	1
1	0	12
2	0	108
3	54	918
4	540	7344
5	5184	57852
6	25173	344925
7	55044	733500
8	9036	90852
9	8	8
Total	95040	1235520

Corollary IV.2: M_{12} and M_{13} both have diameter 9.

Remarkably, only eight permutations of depth 9 exist; the other 95032 were producible by shorter paths. These permutations were as follows:

Path	Permutation
$C12C60798C$	$(0)(7)(8)(15A)(24B)(369)$
$C12C76803C$	$(0)(7)(8)(1A5)(2B4)(396)$
$C02C59A13C$	$(1)(5)(A)(078)(2B4)(369)$
$C02C56A13C$	$(1)(5)(A)(087)(24B)(396)$
$C01C46B23C$	$(2)(4)(B)(15A)(078)(396)$
$C01C49B23C$	$(2)(4)(B)(087)(1A5)(369)$
$C01C436B9C$	$(3)(6)(9)(078)(1A5)(24B)$
$C01C64932C$	$(3)(6)(9)(087)(15A)(24B)$

As is apparent, each of these permutations decomposes into separate actions on the four sets $L'_3 = \{0, 7, 8\}$, $L'_6 = \{1, 5, A\}$, $L'_9 = \{2, 4, B\}$, $L'_C = \{3, 6, 9\}$ — the other three points on each of the four lines of P_3 through the point C. Together with the identity, they constitute a subgroup $N < M_{12}$,

isomorphic to the abelian group $(\mathbf{Z}/3\mathbf{Z})^2$. It will be observed that any two distinct elements of N have the same action on exactly one of the 3-sets L_i'. Thus N is isomorphic to the tetracode [4, p. 81].

The nine elements of N are "antipodal," i.e., at maximal distance not only from the identity but from each other, because N is a group: $d(a, b) = 9$ for $a, b \in N$, $a \neq b$, since $ab^{-1} \in N \setminus \{1\}$ has depth 9. As one consequence, we can partition M_{12} into the $95040/9 = 10560$ left cosets of N and observe that the distance between two distinct elements $x, y \in M_{12}$ is maximal (i.e., 9) if and only if they lie in the same left coset (since $y = xn$ for some $n \in N \setminus \{1\}$, so $d(x, y) = D(x^{-1}y) = D(n) = 9$).

Knowing the diameter of M_{13} provides us with an algorithm for "solving" the Conway game, i.e., finding a move between any two positions $P, P' \in M_{13}$. If $d(P, P') = 9$, then the desired move will be an element of the tetracode group N, so this possibility can be dealt with in at most nine trials. Otherwise, there must be some position at distance ≤ 4 from both P and P' (specifically, the position reached halfway along the move between P and P'). So we list all positions at distance ≤ 4 from P, as well as all those at distance ≤ 4 from P', merge the two lists and check for duplicates. From Theorem IV.1, there are only 8383 positions for each of P and P', so this algorithm is computationally much more efficient than searching through all 1235520 elements of $2M_{13}$.

4 M_{13} and Sextuple Transitivity

Conway's assigning the name "M_{13}" to the quasigroup of all moves in the game is intended to suggest that it exhibits certain properties akin to the "legitimate" Mathieu groups. One natural question is whether M_{13} is sextuply transitive. That is, given any six counters and six points of the projective plane, can an element of M_{13} be found which moves the six counters to the six points in order? (After all, M_{13} has thirteen times as many elements as M_{12}, which acts quintuply transitively on a set of twelve points and appears inside M_{13} as the stabilizer of the hole.) Since M_{13} is not a group, the question actually has two distinct parts, depending on whether we choose the six counters or the six points first. We examine each approach in turn. In both cases, the results of MAKE–M13 were invaluable as a source of ed-

ucated guesses about sextuple transitivity, which could then be proven or disproven independently.

4.1 Sextuple Transitivity On Counters

Let $S = \{X_1, \ldots, X_6\}$ be the set of six counters initially located at positions $p_1, \ldots, p_6$ respectively. We will say that S is "6-transitive" (abbreviated 6T) if for any ordered sextuple $(j_1, \ldots, j_6)$ of points of P_3, there exists an element of M_{13} carrying each counter X_i to the corresponding point j_i. Otherwise, S is "non-6-transitive" (to be abbreviated N6T). Note that if we allow the hole to be one of the "counters," then S is automatically 6T, as we can first take the hole to its desired ending point, then choose an element of M_{12} moving the five other counters anywhere, by quintuple transitivity. The remainder of this section is concerned with investigating what happens when six "real" counters are chosen.

Lemma IV.3: S is 6T $\iff$ no two elements of M_{13} carry the counters S to the same positions.

Proof: By the pigeonhole principle, since $|M_{13}|$ = the number of ordered distinct sextuples of $P3$, which is $13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 1235520$.

Theorem IV.4: Any 6-set S is N6T.

Proof: We examine three simple cases first, then show that the general case can be reduced to one of them.

Lemma IV.5: S is N6T if for some $q \in M_{13}$, there is a line L of P_3 which contains the hole and contains no counters of S.

Proof: Any move along L produces a new element of M_{13} in which the counters of S occupy the same positions. Thus S is N6T by Lemma IV.3.□

Lemma IV.6: S is N6T if for some $q \in M_{13}$, there is a line L of P_3 which contains neither the hole nor any counters of S.

Proof: Play q, then move to any point on L. In the resulting position, no counters of S lie on L. Thus S is N6T by Lemma IV.5. □

Lemma IV.7: S is N6T if for some $q \in M_{13}$, there is a line L of P_3 which does not contain the hole and contains exactly one counter $X_i \in S$.

Proof: Play q, then move the hole to the point holding X_i. In the resulting position, L contains the hole but no counters of S. Thus S is N6T by Lemma IV.5. □

For $q = 1$ and any 6-set of counters S, we will find a line satisfying the condition of one of the above lemmas.

Let $L_1, \ldots, L_4$ be the lines incident to point C (the "hole" in the starting position) and define $d_i = |S \cap L_i|$. By Lemma IV.5, we need investigate only those sets S such that $d_i > 0$ for all i. Reindex the lines L_i so that $d_1 \leq d_2 \leq d_3 \leq d_4$. Since $d_1 + d_2 + d_3 + d_4 = |S| = 6$, there are two cases to consider: either $d_1 = d_2 = d_3 = 1$ and $d_4 = 3$, or else $d_1 = d_2 = 2$ and $d_3 = d_4 = 2$.

Case 1: $(d_1, d_2, d_3, d_4) = (1, 1, 1, 3)$. Without loss of generality, assume $j_1 \in L_1,\ j_2 \in L_2,\ j_3 \in L_3,\ j_4, j_5, j_6 \in L_4$.

Subcase 1A: j_1, j_2, j_3 are collinear. The line containing them, M, must intersect L_4 somewhere other than C, since L_1 already contains both C and j_1. Assume without loss of generality that M intersects L_4 at j_6. The lines M and L_4 contain the points $j_1, \ldots, j_5,\ C$ between them, hence either of the two other lines incident to j_6 satisfies the condition of Lemma IV.7. Hence S is N6T.

Subcase 1B: j_1, j_2, j_3 are not collinear. Then the three lines M_1, M_2, M_3, defined by any two of j_1, j_2, j_3, are distinct. Each such line intersects L_4 in a different place, so the following labelling is justified:

$$M_1 = \{j_1, j_2, j_4, x\},$$
$$M_2 = \{j_1, j_3, j_5, y\},$$
$$M_3 = \{j_2, j_3, j_6, z\}.$$

We have produced two lines containing j_4; they are $L_4 = \{j_4, j_5, j_6, C\}$ and $M_1 = \{j_1, j_2, j_4, x\}$. Of the other two lines, the one that does not contain j_3 satisfies the condition of Lemma IV.7. Hence S is N6T.

Case 2: $(d_1, d_2, d_3, d_4) = (1, 1, 2, 2)$. Without loss of generality, assume $j_1 \in L_1,\ j_2 \in L_2,\ j_3, j_4 \in L_3,\ j_5, j_6 \in L_4$.

Let x be the fourth point on L_4, i.e., $L_4 = \{C, j_5, j_6, x\}$. Let M_1, M_2, M_3 be the other three lines incident to x. None of the M_i contains any of C, j_5, j_6, since each intersects with L_3 at x. Thus no matter how the points j_1, j_2, j_3, j_4 are distributed among the M_i, at least one of M_1, M_2, M_3 must contain no more than one of $\{j_1, \ldots, j_6\}$. This M_i satisfies the condition of Lemma IV.7, and so S is N6T. □

4.2 Sextuple Transitivity On Points of P_3

Let $X = \{x_1, \ldots, x_6\}$ be a set of distinct points of P_3. We will employ an abuse of language similar to that of the previous section: X will be called "6-transitive" (6T) if for any ordered sextuple of counters $C = \{c_1, \ldots, c_6\}$, there exists an element of M_{13} taking C to X, i.e., moving each counter c_i to the corresponding point x_i. Otherwise, X is "non-6-transitive" (to be abbreviated N6T).

Lemma IV.8: X is 6T $\iff$ no two distinct elements of M_{13} carry the same ordered 6-tuple of counters to X.

Proof: By the pigeonhole principle, since the number of 6-sets X equals $|M_{13}| = 1235520$ (Lemma IV.3). □

A 6-set X may be described as one of three different types, determined by its geometry as a subset of P_3:

Type I: X contains all the points of some line.

Type II: X is disjoint from some line.

Type III: X is neither of type I or type II. (I.e., X has between one and three points in common with every line of P_3.)

Note that X can neither contain two lines (since the union of two lines contains seven points) nor be of both type I and type II (since the intersection of any two lines is nonempty).

It is informative to count the number of 6-sets of each type. First note that

the total number of 6-sets is $\binom{13}{6} = 1716$. For type-I sets, we choose one of 13 lines and then add 2 of the 9 points not on it, obtaining $13 \cdot \binom{9}{2} = 468$ different sets. For type II, we choose one of 13 lines to be excluded from X and then choose 6 of the 9 points not on it, obtaining $13 \cdot \binom{9}{6} = 1092$. However, any 6-set disjoint from more than one line will be counted twice in this calculation. No 6-set can be disjoint from more than two lines, but the complement of the union of two lines contains exactly six points, implying that there are $\binom{13}{2} = 78$ such 6-sets. Thus the number of 6-sets of type II is $1092 - 78 = 1014$. Finally, there are $1716 - 1014 - 468 = 234$ sets of type III.

We have described type-III sets almost as an afterthought. In fact, determining whether type-III sets are 6T is the most difficult case. We first prove a lemma which neatly describes the geometry of type-III sets, before moving on to a general investigation of sextuple transitivity of points.

Lemma IV.9: Let $X = \{x_1, \ldots, x_6\}$ be a 6-set of type-III. Up to reindexing, each of the triples $\{x_1, x_2, x_3\}$, $\{x_1, x_4, x_5\}$, $\{x_2, x_4, x_6\}$, and $\{x_3, x_5, x_6\}$ is collinear.

Proof: First of all, any 6-set (of whatever type) must contain at least one collinear triple, since there are $\binom{6}{2} = 15$ ways of determining a line from two points of X, and only 13 lines of P_3. So pick three points x_1, x_2, x_3 that lie on a line L, and let c be the fourth point on L. Since each line of P_3 intersects L, we have shown that X contains a point on every line, except for the three other lines L_1, L_2, L_3 incident to c. Since X cannot contain L (being of type III), c itself cannot be an element of X. So X can be only completed if (up to reindexing) $x_4 \in L_1$, $x_5 \in L_2$, $x_6 \in L_3$. However, we must restrict our choice so that x_4, x_5, x_6 are not collinear. (If they are, then the fourth point on the line L' containing them must lie on L. It cannot be c since we would then have two distinct lines, L' and L_1, containing both c and x_4, but if it is x_1, x_2 or x_3, then X contains L' and is not of type III.) Hence we may choose x_4 and x_5 freely (3 choices for each) but then have only two choices for x_6 (we may not pick the point on L_3 collinear with x_4 and x_5). Now, the line containing x_4 and x_5 must intersect L. The intersection cannot be c, so must be some x_i. Reindex so that it is x_1. By analogous arguments, and reindexing appropriately, we can conclude that the triples $\{x_2, x_4, x_6\}$ and $\{x_3, x_5, x_6\}$ are collinear, as desired. □

Note that the list of type-III sets obtained in this way has $13 \cdot \binom{4}{3} \cdot 3 \cdot 3 \cdot 2 = 936$ elements. However, any type-III set X will appear four times in the list —

once for each of the lines containing three points of X — and so the number of distinct type-III sets enumerated thusly is $936/4 = 234$, which agrees with our original counting.

We note in passing that Lemma IV.9 doubles as a uniqueness proof for P_3, since we have been able to construct all thirteen points and lines, unique up to labelling, starting with only the combinatorial properties of the projective plane. Moreover, we can count the automorphisms of P_3, based on the fact that choosing any type-III set determines the geometry of the remaining seven points. There are 234 sets of type III (as shown above). Each such set S has $4! = 24$ automorphisms, corresponding to the possible permutations of the four lines through three elements of S. Therefore P_3 has $234 \cdot 24 = 5616$ automorphisms. This agrees with our definition of P_3 as the space $F_3^3 \setminus \{(0,0,0)\}$ modulo the relation $x = -x$. The general linear group $GL_3(3)$ has $(3^3-1)(3^3-3)(3^3-3^2) = 26 \cdot 24 \cdot 18 = 11232$ elements [7, p. 162]. The group of automorphisms of P_3 is the projective linear group $PGL_3(3)$, which is the quotient of $GL_3(3)$ by the group N of maps $x \mapsto kx$. Since the only possible values for k are ± 1, the group N is cyclic of order 2 and $|\,PGL_3(3)| = |\,GL_3(3)|/2 = 11232/2 = 5616$, as desired.

Theorem IV.10: Any 6-set $X = \{x_1, \ldots, x_6\}$ is 6T if and only if it is of type I.

Proof: We examine the three types of 6-set separately.

Case 1: X is of type I.

Let $L = \{x_1, x_2, x_3, x_4\}$ be the (unique) line contained in X. The other two points x_5 and x_6 determine a unique line M, which in turn intersects L in a unique point. Without loss of generality, assume that this point is x_1. Let n be the fourth point on M.

Now, let $C = \{c_1, \ldots, c_6\}$ be any 6-tuple of counters. Play a move σ as follows: first move the hole to x_1, then play a move which fixes the hole at x_1 and moves counter c_j to point x_j for $j = 2, \ldots, 6$. (Such a move must exist by quintuple transitivity of M_{12}). Let p be the point to which σ moves c_1. If $p \neq n$, then the line through p and x_1 does not pass through any of $x_2, \ldots, x_6$, so we can obtain a permutation taking C to X by first playing σ, then moving the hole from x_1 to p.

If $p = n$, then we must do a little more work. By first playing σ, then moving

the hole along the path $x_1x_2nx_3x_4n$, we obtain the desired permutation taking C to X.

Case II: X is of type II.

Let L be a line of P_3 disjoint from X. Start by moving the hole to some point in L. By then moving the hole to any other point of L, a new element of M_{12} is obtained which carries the same 6-set of counters to X, since the last move does not change any of the counters lying on X. Hence X is N6T by Lemma IV.8.

Case III: X is of type III.

Recall Lemma IV.10, which describes the geometry of X. To complete our labelling of P_3, let c_1, c_2, c_3, c_4 denote the fourth points on the lines containing $\{x_1, x_2, x_3\}$, $\{x_1, x_4, x_5\}$, $\{x_2, x_4, x_6\}$, and $\{x_3, x_5, x_6\}$ respectively. Now consider the lines of P_3 containing the pairs $\{x_1, x_6\}$, $\{x_2, x_5\}$, and $\{x_3, x_4\}$. None of these lines can contain any other x_i, or any of the c_i. Since any two of the lines intersect in a point, they can be written as $\{x_1, x_6, d_2, d_3\}$, $\{x_2, x_5, d_1, d_3\}$, and $\{x_3, x_4, d_1, d_2\}$. We have now accounted for all thirteen points of P_3: they are

$$\{x_1, \ldots, x_6,\ c_1, \ldots, c_4,\ d_1, \ldots, d_3\}.$$

We have also described seven of the thirteen lines, to wit:

$$\begin{array}{ll} \{x_1, x_2, x_3, c_1\}, & \{x_1, x_6, d_2, d_3\}, \\ \{x_1, x_4, x_5, c_2\}, & \{x_2, x_5, d_1, d_3\}, \\ \{x_2, x_4, x_6, c_3\}, & \{x_3, x_4, d_1, d_2\}, \\ \{x_3, x_5, x_6, c_4\}. & \end{array}$$

The other six lines must therefore be

$$\begin{array}{ll} \{x_1, d_1, c_3, c_4\}, & \{x_2, d_2, c_2, c_4\}, \\ \{x_3, d_3, c_2, c_3\}, & \{x_4, d_3, c_1, c_4\}, \\ \{x_5, d_2, c_1, c_3\}, & \{x_6, d_1, c_1, c_2\}. \end{array}$$

Suppose that the initial position of the hole is c_1. Then the permutations

$$(c_1\ d_3\ x_5)(d_2\ c_3)(x_2\ d_1)$$

and

$$(c_1\ d_1\ x_2\ d_2)(x_5\ c_3\ d_3)(c_2\ c_4),$$

produced by paths $c_1x_5x_3$ and $c_1d_2x_2d_1$ respectively, both take the counters originally located at $(x_1, d_1, x_3, x_4, d_3, x_6)$ to the positions $(x_1, \ldots, x_6)$ respectively. Hence X is N6T.

If, on the other hand, the hole is initially located at some x_i or some d_i, we can simply make an initial move which takes the hole to c_1, then proceed as above.

5 Adding A Sign To The Conway Game

The following argument, which is due to Elkies [6], shows that the signed extension of the Conway game mentioned earlier produces the group $2M_{12}$. In the process, we note certain facts about the geometry of the projective plane P_3. A corollary of Elkies' result is that the original Conway game group G_C is a subgroup of M_{12}; combined with the earlier construction of M_{12} from particular elements of G_C, this completes the verification that $G_C = M_{12}$.

Let X be the vector space F_3^{13}, with basis vectors $\{x_p\},\ p \in P_3$. We shall adopt the notational convention that a vector $v \in X$ has coordinates v_p, i.e., $v = \sum_p v_p x_p$.

Define the code C to be the vector subspace of X spanned by the vectors

$$h_l = \sum_{p \in l} x_p$$

for all lines l of P_3. We make use of the following definitions: the *support* of a codeword c is $\mathrm{Supp}(c) = \{p \in P_3\ :\ c_p \neq 0\}$, and the *weight* of c is $\mathrm{wt}(c) = |S(c)|$.

The following theorem gives several useful tools for working with C.

Theorem IV.11: For any $c \in C$, the following properties hold:

1. $$\sum_{p \in P_3} (c_p^2) = \left(\sum_{p \in P_3} c_p \right)^2 . \qquad (*)$$

2. $\mathrm{wt}(c) \equiv 0$ or $1 \pmod 3$.

3. $\mathrm{wt}(c) \equiv 0 \pmod 3$ iff
$$\sum_{p \in P_3} c_p = 0.$$

4. The set $C_0 = \{c \in C \ : \ \mathrm{wt}(c) \equiv 0 \pmod 3\}$ is a vector space whose codimension in C (i.e., $\dim(C) - \dim(C_0)$) equals 1.

5. For any line l of P_3,
$$\sum_{p \in P_3} c_p = \sum_{p \in l} c_p. \qquad (**)$$

6. C_0 is the dual space of C under the canonical scalar product
$$c \cdot d = \sum_{p \in P_3} c_p d_p.$$

7. $\dim(C) = 7$ and $\dim(C_0) = 6$.

8. The minimal weights of C and C_0 are 4 and 6 respectively.

Proof:

1. Since the h_l span C, it suffices to prove the identity
$$\sum_{p \in P_3} (c_p c'_p) = \left(\sum_{p \in P_3} c_p \right) \left(\sum_{p \in P_3} c'_p \right)$$
for $c = h_l$, $c' = h_m$. In this case, both sides of the equation collapse to 1, whether l and m are the same or different.

2.
$$\mathrm{wt}(c) = \sum_{p \in P_3} (c_p^2) = \left(\sum_{p \in P_3} c_p \right)^2$$
is a square in F_3, hence is congruent to either 0 or 1 (mod 3).

3. $c \in C_0$ if and only if the right side of (*), and thus $\mathrm{wt}(c)$, are congruent to 0 (mod 3). Otherwise, $\mathrm{wt}(c) = 1$.

4. By (3), C_0 is a subgroup of C (considered as an abelian group under addition); its cosets are $\{c \in C : \sum_p c_p \equiv j \pmod 3\}$ for $j = 0, 1, 2$. So $[C : C_0] = 3$, and since C and C_0 are vector spaces over F_3, the space C_0 has codimension 1.

5. Since (**) is a linear identity, it suffices to verify it for the generators $\{h_l\}$. Let $c = h_m$; then both sides of (**) are equal to 1 whether l and m are the same or different.

6. (**) generalizes to the bilinear identity
$$c \cdot c' = \sum_{p \in P_3} c_p c'_p = \left(\sum_{p \in P_3} c_p \right) \left(\sum_{p \in P} c'_p \right).$$
If $c \in C_0$, then the right-hand side of the above equation is zero for any $c' \in C$. Therefore $C \subset C_0^\perp$. To prove the reverse inclusion, let $w \in C_0^\perp$. If $\mathrm{Supp}(w)$ intersects any line l in more than 2 points, then it is possible to reduce $\mathrm{wt}(w)$ by adding or subtracting h_l from w. Repeating this process as many times as needed, we obtain $w' \in C_0^\perp$ congruent to w modulo C (since $h_l \in C \subset C_0^\perp$) and such that $\mathrm{Supp}(w')$ intersects no line in more than two points.

   We claim that $\mathrm{Supp}(w') = \emptyset$. By inspection, we can see that $\mathrm{wt}(w') \leq 4$: let $Z = \{p_1, p_2, p_3, p_4\}$ be four points of P_3, no three on any one line. Let us list all other points on the lines joining any two points of Z. This list will contain twelve points, including three duplicates, hence nine different points not contained in Z. Thus we have accounted for all thirteen points of P_3, and there is no way to add a fifth point to Z without intersecting some line three times. However, if $0 < \mathrm{wt}(w') < 5$, then there exists some line l disjoint from $\mathrm{Supp}(w')$ and another line m intersecting it in exactly one point. But then the difference of h_l

and h_m is in C_0 but is not orthogonal to w, which is a contradiction since $C \subset C_0^{\perp}$. Hence $\mathrm{Supp}(w') = \emptyset, w' = 0$, and $w \in C$, completing the proof. (Elkies' proof used the fact [1, p. 18] that if n is odd, the projective plane of order n contains no hyperovals, i.e., sets of $n+2$ points no three of which are collinear. The argument here, however, is more elementary, and independent of that theorem.)

7. By (6),

$$\dim(C_0) + \dim(C_0^{\perp}) = 13 = \dim(C) - 1 + \dim(C),$$

and so $\dim(C_0) = 6$ and $\dim(C) = 7$.

8. C contains codewords of weight 4, the generators c_l. By the preceding argument, if $w \in C$ and $\mathrm{Supp}(w)$ meets each line of P_3 in two points or fewer, then $w = 0$. In particular, C has no words of weight 1 or 2. Moreover, if $w \in C$ has weight 3, then the three points of $\mathrm{Supp}(w) = 3$ must all lie on some line l. But then the weight of w can be reduced by adding or subtracting h_l, which, as we have seen, leads to a contradiction. Thus C has minimal weight 4. Since $C_0 \subset C$ and the weight of any word of C_0 is a multiple of 3, C_0 has minimal weight at least 6, which is realized by any difference $h_l - h_m$ of distinct generators. □

For each $p \in P_3$, define a subcode $\mathcal{G}_p = \{c \in C \ : \ c_p = -\sum_{q \in P_3} c_q\}$, and let $\mathbf{G}_p$ be the restriction of $\mathcal{G}_p$ to $P_3 - \{p\}$.

Proposition IV.12: $\mathbf{G}_p$ is isomorphic to the Golay code C_{12} for any $p \in P_3$.

Proof: $\mathcal{G}_p$ is a proper subspace of C, since no h_l lies in $\mathcal{G}_p$. However, for any $v \in C$, exactly one of v, $v + h_l$, $v - h_l$ lies in $\mathcal{G}_p$, so $\dim(\mathcal{G}_p) = 6$. The restriction map $\phi \ : \ \mathcal{G}_p \to \mathbf{G}_p$ can have only vectors of weight ≤ 1 in its kernel. Since 0 is the only such vector, ϕ must be a bijection, and $\dim(\mathbf{G}_p) = \dim(\mathcal{G}_p) = 6$. □

If $c \in \mathcal{G}_p$, the weight of $\phi(c)$ is congruent (mod 3) to

$$\sum_{q \neq p} (c_q^2) \ = \ \left(\sum_{q \in P_3} c_q^2 \right) - c_p^2 \ = \ \left(\sum_{q \in P_3} c_q \right)^2 - c_p^2 \ = \ 0.$$

The generalized bilinear version of the above identity, for any $c, d \in \mathcal{G}_p$, is

$$\phi(c)\cdot\phi(d) \;=\; \sum_{q\neq p} c_q d_q \;=\; \sum_{q\in P_3}(c_q d_q - c_p d_p) \;=\; \left(\sum_{q\in P_3} c_q\right)\left(\sum_{q\in P_3} d_q\right) - c_p d_p$$
$$=\; (-c_p)(-d_p) - c_p d_p \;=\; 0.$$

Hence the code $\mathbf{G}_p$ is self-dual. We have proven that $\mathbf{G}_p$ is a ternary self-dual code in which the weight of every codeword is a multiple of 3 and whose minimal weight is ≥ 3; it follows that $\mathbf{G}_p$ is isomorphic to the Golay code C_{12} [4, p. 434]. □

Now, let $l = \{p, q, r, s\}$ be a line of P, and define a linear transformation $\tilde{\iota}_{pq} : F_3^{13} \to F_3^{13}$ taking w to w', where

$$w'_p = w_q,\; w'_q = -w_p - w_q,\; w'_r = -w_s,\; w'_s = -w_r,$$

and $w'_t = w_t$ for all $t \notin l$. ($\tilde{\iota}_{pq}$ represents a move in the signed Conway game, moving the hole from p to q and interchanging and flipping the counters on r and s.)

Proposition IV.13: $\tilde{\iota}_{pq}(\mathcal{G}_p) = \mathcal{G}_q$.

Proof: It suffices to prove the inclusion $\tilde{\iota}_{pq}(\mathcal{G}_p) \subset \mathcal{G}_q$, for then $\tilde{\iota}_{qp}(\mathcal{G}_q) \subset \mathcal{G}_p$ and $\tilde{\iota}_{pq}(\tilde{\iota}_{qp}(\mathcal{G}_q)) = \mathcal{G}_q \subset \tilde{\iota}_{pq}(\mathcal{G}_p)$.

Let $c \in \mathcal{G}_p, c' = \tilde{\iota}_{pq} c$. First note that

$$c_p \;=\; -\sum_{q\in P} c_q \;=\; -\sum_{q\in l} c_q$$
$$=\; -c_p - c_q - c_r - c_s$$

which implies that $c_p = c_q + c_r + c_s$. Now,

$$c - c' \;=\; \sum_{p\in l}(c_p - c'_p)x_p$$

$$= (c_p - c_q)x_p + (c_p - c_q)x_q + (c_r + c_s)x_r + (c_r + c_s)x_s$$
$$= (c_p - c_q)h_l.$$

So $c - c' \in C$, whence $c' \in C$. Moreover,

$$\sum_{p \in P} c'_p \;=\; \sum_{p \in l} c'_p \;=\; c'_p + c'_q + c'_r + c'_s$$
$$=\; c_q - c_p - c_q - c_s - c_r \;=\; c_p + c_q \;=\; -c'_q.$$

Therefore, $c' \in \mathcal{G}_q$. □

Corollary IV.14: Any element of the "signed Conway game group" G_C^+ — i.e., a permutation of $P - \{p\}$ induced by some move $\tilde{\iota}_{zp}\tilde{\iota}_{yz} \ldots \tilde{\iota}_{pq}$ — is an automorphism of the Golay code $\mathbf{G}_p$.

It follows that G_C^+ is a subgroup of the automorphism group of the Golay code, which is the group $2M_{12}$ of Part III. G_C^+ in fact contains a central involution -1, which flips every counter in its place, and taking the quotient group of G_C^+ by $\{\pm 1\}$ is equivalent to ignoring flips. That is, the resulting group is the original Conway game group G_C. Therefore, since $G_C^+ < 2M_{12}$, it follows that $G_C < M_{12}$. We know from MAKE–M13 and the constructions of IV.2 that the reverse inclusion holds. This completes the verification that $G_C = M_{12}$.

6 Distance in $2M_{13}$

The metric described in IV.2 extends without modification on $2M_{13}$. To facilitate the work that follows, we converted MAKE–M13 into a new program MAKE–2M13 (Appendix 2), which keeps track of flips. It turns out that the addition of a sign imparts some new metric properties to the Conway game. The proof of the following theorem, like that of Theorem IV.1, is empirical, using the results of MAKE–2M13.

Theorem IV.15: The depth distributions of $2M_{12}$ and $2M_{13}$ are as follows:

Depth	Permutations in $2M_{12}$	Permutations in $2M_{13}$
0	1	1
1	0	12
2	0	108
3	54	918
4	540	7344
5	5184	57852
6	25821	356949
7	85230	1192770
8	72351	843291
9	898	11674
10	0	108
11	0	12
12	1	1
Total	190080	2471040

Corollary IV.16: $2M_{12}$ and $2M_{13}$ have diameter 12.

The unique element of M_{13} at depth twelve is -1, the central involution flipping each counter without moving it. (There are, of course, many different length-12 paths that produce -1.) By extension, two elements $a, b \in 2M_{13}$ are *antipodal*, i.e., at maximal distance from each other, iff $a = -b$.

Since every permutation has a unique antipode, we can visualize $2M_{13}$ as a "globe" in which pairs of poles represent antipodal permutations. The distribution of depths lends this image further credence.

In particular, the depth distributions of $2M_{12}$ and $2M_{13}$ can be described as "symmetric near the poles": for $k \leq 2$, there are equal numbers of permutations at depths k and $12 - k$. However, this symmetry breaks down further from the poles — more elements of $2M_{13}$ lie at depth $12 - k$ than at k for $3 \leq k \leq 5$. One explanation for this phenomenon is as follows: if $x \in 2M_{13}$ lies at depth d, then $-x$ must lie at depth *at least* $12-d$, otherwise $-1 = x(-x)^{-1}$ could be produced by a path of length $< d + (12 - d) = 12$, which we know empirically to be false. However, the depth of $-x$ will be *exactly* $12-d$ only when some path from d to $-d$ has the identity as one of its intermediate positions, which need not be the case. Moreover, if $D(x) = k$ for $x \in 2M_{12}$, then the two lifts of x in $2M_{13}$, $\tilde{x}$ and $-\tilde{x}$, have depth $\geq k$, with equality holding for at least one of the two. Thus, e.g., if $D(x) > 6$,

then $D(\tilde{x}) + D(-\tilde{x}) > 12$.

On the other hand, the symmetry for $k \leq 2$ can in part be explained theoretically; we can show at least that the negative of a permutation at depth 1 or 2 must be at depth 11 or 10, respectively. We must rely on MAKE–2M13 for the converse, however.

Lemma IV.17: $d(x, y) = d(-x, -y)$.

Proof: $d(-x, -y) = D((-x)^{-1}(-y)) = D(x^{-1}y) = d(x, y)$.

Proposition IV.18: If $D(x) \leq 2$, then $D(-x) = 12 - D(x)$.

Proof: Define $T = \{x \in 2M_{13} : D(x) = k\}$ and let $-T = \{-x : x \in T\}$, which is the same as $\{x : d(x, -1) = k\}$ by Lemma IV.17. If $k \leq 2$, then all permutations in T are isomorphic, i.e., any pair can be put in correspondence under an appropriate isomorphism of P_3. Thus their negatives in $-T$ are isomorphic as well. In particular, all elements of $-T$ lie at the same depth. But for -1 to lie at depth 12, at least one element of $-T$ must lie at depth $12 - k$. □

Notice that this argument fails for $k > 2$, since there exist nonisomorphic elements whose depths are equal but greater than 2. (E.g., there are elements of both M_{12} and $M_{13} \backslash M_{12}$ at depth 3.) Furthermore, G_C^+ has many elements at depth 9 other than the negatives of permutations of depth 3 (which are at distance 3 from -1) and the lifts of antipodal elements in M_{12}. A classification of all such elements, as well as deeper investigation of the cycle-shapes of permutations appearing at various depths in both M_{13} and $2M_{13}$, awaits further research.

References

[1] P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and their Links*. Cambridge: Cambridge Univ. Press, 1991.

[2] Robin J. Chapman, "An Elementary Proof of the Simplicity of the Mathieu Groups M_{11} and M_{23}", *American Mathematical Monthly* 102 (June-July 1995), pp. 544–5.

[3] John H. Conway, "Graphs and Groups and M_{13}", *Notes from New York Graph Theory Day XIV* (1987), pp. 18–29.

[4] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed. (New York: Springer-Verlag, 1993).

[5] Philip J. Greenberg, *Mathieu groups*. New York: Courant Inst., 1973.

[6] Noam D. Elkies, "The double cover of Conway's 'M_{13}' ", unpublished paper, 1994.

[7] Joseph J. Rotman, *An Introduction to the Theory of Groups*, 3rd ed. Boston: Allyn and Bacon, 1984.