THE MATHIEU GROUP M_{12} AND ITS PSEUDOGROUP EXTENSION M_{13}

JOHN H. CONWAY, NOAM D. ELKIES, AND JEREMY L. MARTIN

ABSTRACT. We study a construction of the Mathieu group M_{12} using a game reminiscent of Loyd's "15-puzzle". The elements of M_{12} are realized as permutations on 12 of the 13 points of the finite projective plane of order 3. There is a natural extension to a "pseudogroup" M_{13} acting on all 13 points, which exhibits a limited form of sextuple transitivity. Another corollary of the construction is a metric, akin to that induced by a Cayley graph, on both M_{12} and M_{13}. We develop these results, and extend them to the double covers and automorphism groups of M_{12} and M_{13}, using the ternary Golay code and 12×12 Hadamard matrices. In addition, we use experimental data on the quasi-Cayley metric to gain some insight into the structure of these groups and pseudogroups.

1. INTRODUCTION

Sam Loyd's classic *15-puzzle* consists of 15 numbered tiles placed in a 4×4 square grid, with one square, the *hole*, left empty. To solve the puzzle, one slides the tiles around the grid until they are in a specified order. Each sequence of slides induces a permutation in the symmetric group $\mathfrak{S}_{16}$. The permutations arising from *closed* sequences of slides—that is, sequences that return the hole to its initial location—form a subgroup of the symmetric group $\mathfrak{S}_{15}$, with the group operation given by concatenation of sequences. This subgroup is known to be the alternating group $\mathfrak{A}_{15}$ (see [Archer:1999]).

We study an analogous game, first mentioned in [Conway:1987], in which the 4×4 grid of Loyd's puzzle is replaced by $\mathbb{P}_3$, the projective plane of order 3. In the "basic game", we place numbered counters on 12 of the 13 points of $\mathbb{P}_3$, leaving a hole at the thirteenth point. The elementary move, analogous to sliding an adjacent tile to the empty square in Loyd's puzzle, is a double transposition taking place in a line containing the hole. The *basic $\mathbb{P}_3$-game group* G_{bas} consists of the permutations of the 12 counters coming from closed move sequences. We shall prove that G_{bas} is isomorphic to the Mathieu group M_{12}.

We give the name M_{13} to the set of permutations induced by arbitrary (not necessarily closed) move sequences. This is a subset of $\mathfrak{S}_{13}$, but is not a group, because concatenation of arbitrary move sequences is not always allowed. Specifically, a move sequence moving the hole from p to q may be followed by one taking the hole from r to s if and only if $q = r$.

2000 *Mathematics Subject Classification.* Primary 20B25; Secondary 05B25, 51E20, 20B20.

Key words and phrases. Mathieu group, finite projective plane, Golay code, Hadamard matrix.

Second author supported in part by the Packard Foundation and the National Science Foundation. Third author supported in part by an NSF Postdoctoral Fellowship.

The $\mathbb{P}_3$-game can be extended in two ways. First, we can make the counters two-sided and modify the definition of a move to flip certain counters. We study this "signed game" in Section 3. The group G_{sgn} resulting from this change is the nontrivial double cover $2M_{12}$ of the Mathieu group (see [Conway:1985, pp. 31–32]), realized as the automorphism group of the ternary Golay code $\mathscr{C}_{12}$. The set $2M_{13}$ of all reachable signed permutations is thus a double cover of M_{13}.

A second way to extend the basic game is to place a second set of counters on the lines of $\mathbb{P}_3$. We study this "dualized game" in Section 4. This approach yields another proof (using Hadamard matrices) that the group G_{bas} is isomorphic to M_{12}; in addition, we obtain a concrete interpretation of an outer automorphism of M_{12}.

M_{12} is unique among groups in having a faithful and sharply quintuply transitive action on a 12-element set. Our construction of M_{13} suggests the following question: does M_{13} have a sextuply transitive "action" on the 13-element set $\mathbb{P}_3$? In general, the answer is no, but M_{13} does exhibit some limited forms of sextuple transitivity, which we describe in Section 5.

In Section 6, we study the quasi-Cayley metric on M_{12} and its extensions, in which the distance $d(\sigma, \tau)$ between two permutations is the minimum number of moves of the basic or signed game needed to realize $\sigma^{-1}\tau$. We programmed a computer to generate lists of all positions of each of the versions of the $\mathbb{P}_3$-game. The data in these lists provides a starting point for investigation of various aspects of the structure of the groups and pseudogroups. For instance, the 9-element *tetracode* (see, e.g., [Conway:1999, p. 81]) appears as the subgroup of M_{12} consisting of the starting position of the basic game, together with the 8 positions at maximal distance from it.

The construction of M_{13} was first given by the first author in [Conway:1987]; see also [Conway:1997]. The latter article includes some examples of analogous "games" played on geometric structures other than $\mathbb{P}_3$. It would be interesting to look for further examples along these lines.

Much of the material of this paper comes from the third author's undergraduate thesis [Martin:1996], written under the direction of the second author.

2. The basic and signed $\mathbb{P}_3$-games

2.1. **Finite projective planes.** We begin by reviewing the definitions and facts we will need concerning $\mathbb{P}_3$.

Let $\mathcal{P} = \{p, q, \dots\}$ be a finite set of points and $\mathcal{L} = \{\ell, m, \dots\}$ be a finite set of lines. Each line may be regarded as a set of points; we write $\mathcal{L}(p)$ for the set of lines containing a point p.

Definition 2.1. Let $n \geq 2$. The pair $(\mathcal{P}, \mathcal{L})$ is a *projective plane of order n* if the following conditions hold:

(1) $|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1$.
(2) $|\mathcal{L}(p)| = |\ell| = n + 1$ for every $p \in \mathcal{P}$ and $\ell \in \mathcal{L}$.
(3) Two distinct points p, q determine a unique line $\overline{pq}$, that is, $\mathcal{L}(p) \cap \mathcal{L}(q) = \{\overline{pq}\}$.
(4) Two distinct lines ℓ, m determine a unique point, that is, $|\ell \cap m| = 1$. (We often write $\ell \cap m$ for the unique intersection point.)

The most familiar example of a finite projective plane is the *classical projective plane* $\mathbb{P}^2(\mathbb{F}_n)$, where n is a prime power. This projective plane is defined as follows. Let $\mathbb{F}_n$ be the a field of n elements, and let $\mathcal{P}$ and $\mathcal{L}$ be respectively the sets of 1- and 2-dimensional vector subspaces of $(\mathbb{F}_n)^3$, with incidence given by inclusion. Then $\mathbb{P}^2(\mathbb{F}_n) = (\mathcal{P}, \mathcal{L})$ is a projective plane of order n.

An *oval* (resp. *hyperoval*) in a projective plane of order n is a set of $n+1$ (resp. $n+2$) points, no three of which are collinear. For example, a smooth conic in a classical projective plane is an oval. Also, there is no such thing as a "hyperhyperoval", for the following reason. Let S be a set of $n+3$ or more points in a projective plane of order n, and $p \in S$. There are $n+1$ lines containing p, so by the pigeonhole principle there exist two distinct points in $S \setminus \{p\}$ which are collinear with p.

For the rest of the paper, we shall be exclusively concerned with the classical projective plane $\mathbb{P}^2(\mathbb{F}_3)$, and will use the abbreviated notation $\mathbb{P}_3$ for this plane. Note that $\mathbb{P}_3$ has 13 points, each lying on 4 lines, and 13 lines, each containing 4 points. By elementary counting, $\mathbb{P}_3$ has $13 \cdot 12 \cdot 9 \cdot 4 = 5616$ ordered ovals.

Proposition 2.2. (1) *Up to isomorphism,* $\mathbb{P}_3$ *is the unique finite projective plane of order* 3.
(2) *The automorphism group* $\mathrm{Aut}(\mathbb{P}_3)$ *acts sharply transitively on ordered ovals; in particular,* $|\mathrm{Aut}(\mathbb{P}_3)| = 13 \cdot 12 \cdot 9 \cdot 4 = 5616$.
(3) $\mathbb{P}_3$ *contains no hyperovals.*

These facts are well known (see, e.g., [Cameron:1991]). We prove them here by constructing an explicit labelling for the points and lines of $\mathbb{P}_3$, which we will use in the proofs of Proposition 3.1 and Theorem 5.3.

Proof. Let $\mathbb{P}_3$ be a projective plane of order 3. Let $O = (q_1, q_2, q_3, q_4)$ be an ordered oval in $\mathbb{P}_3$. We will show that each point and each line of $\mathbb{P}_3$ is determined uniquely as a function of q_1, q_2, q_3, q_4. This will show that if $\mathbb{P}'_3$ is any other projective plane of order 3, and (q'_1, q'_2, q'_3, q'_4) is an ordered oval in $\mathbb{P}'_3$, then there is a unique isomorphism from $\mathbb{P}_3$ to $\mathbb{P}'_3$ sending (q_1, q_2, q_3, q_4) to (q'_1, q'_2, q'_3, q'_4). In particular, it will follow that all projective planes of order 3 are isomorphic, with an automorphism group of order $13 \cdot 12 \cdot 9 \cdot 4$. We already know one, namely the classical projective plane over $\mathbb{F}_3$; and we know that its automorphism group contains $\mathrm{PGL}_3(\mathbb{F}_3)$, a group of order $(26 \cdot 24 \cdot 18)/2 = 13 \cdot 12 \cdot 9 \cdot 4$. Hence $\mathbb{P}_3$ is the unique projective plane of order 3, and $\mathrm{PGL}_3(\mathbb{F}_3)$ is its full automorphism group. Along the way, we will show that $\mathbb{P}_3$ has no hyperovals.

The points of $\mathbb{P}_3$ include:

- the four points q_1, q_2, q_3, q_4;
- the three points $r_1 = \overline{q_1 q_2} \cap \overline{q_3 q_4}$, $r_2 = \overline{q_1 q_3} \cap \overline{q_2 q_4}$, $r_3 = \overline{q_1 q_4} \cap \overline{q_2 q_3}$; and
- the six points s_{ij} $(1 \le i < j \le 4)$ lying on just one of the secant lines $\overline{q_i q_j}$ to O.

(Recall that a *secant* to an oval is a line determined by two of its points; thus each secant $\overline{q_i q_j}$ to O contains two q_i's, one r_i, and one other point, which we call s_{ij}.) This accounts for all $4 + 3 + 6 = 13$ points, and in particular shows that there are no hyperovals.

We have accounted for six lines, namely the secants to O. There are also the four *tangents* to O, the lines which pass through exactly one of its points. The tangent to O at q_1 intersects each of the lines $\overline{q_2 q_3}$, $\overline{q_2 q_4}$, $\overline{q_3 q_4}$ in a point not on any other

secant, which is that line's fourth point. We have thus identified the 4 points on each tangent. Three additional lines remain to be identified.

We claim that r_1, r_2, r_3 are not collinear, and thus that the lines through pairs in r_1, r_2, r_3 complete the roster of lines of $\mathbb{P}_3$. Consider for instance s_{12}, the fourth point on $\overline{q_1 q_2}$. It lies also on the tangents at q_3 and q_4. The points on these three lines are: s_{12} itself; q_1, q_2, r_1; q_3, s_{14}, s_{24}; q_4, s_{13}, s_{23}. Hence the remaining line through s_{12} goes through r_2, r_3, and s_{34}. This identifies the line $\overline{r_2 r_3}$ and shows that it does not contain r_1. Likewise, we find that the line $\overline{r_1 r_2}$ contains s_{14} and s_{23}, while $\overline{r_1 r_3}$ contains s_{13} and s_{24}.

We have now identified all 13 points and all 13 lines of $\mathbb{P}_3$ and their incidence relation, as desired. To summarize, the lines are:

$$\begin{array}{lll} \{q_1,\, q_2,\, r_1,\, s_{12}\}, & \{q_1,\, s_{23},\, s_{24},\, s_{34}\}, & \{r_1,\, r_2,\, s_{14},\, s_{23}\}, \\ \{q_1,\, q_3,\, r_2,\, s_{13}\}, & \{q_2,\, s_{13},\, s_{14},\, s_{34}\}, & \{r_1,\, r_3,\, s_{13},\, s_{24}\}, \\ \{q_1,\, q_4,\, r_3,\, s_{14}\}, & \{q_3,\, s_{12},\, s_{14},\, s_{24}\}, & \{r_2,\, r_3,\, s_{12},\, s_{34}\}, \\ \{q_2,\, q_3,\, r_3,\, s_{23}\}, & \{q_4,\, s_{12},\, s_{13},\, s_{23}\}, & \\ \{q_2,\, q_4,\, r_2,\, s_{24}\}, & & \\ \{q_3,\, q_4,\, r_1,\, s_{34}\}. & & \end{array} \tag{2.1}$$

□

The definition of $\mathbb{P}_3$ is *self-dual* in the sense that interchanging the terms "point" and "line" preserves the definition. One can label the points by $\{0, 1, \ldots, 12\}$ and the lines by $\{\overline{0}, \overline{1}, \ldots, \overline{12}\}$ such that the lines containing the point x have the same labels as the points of the line $\overline{x}$. For future reference, we give one such labelling:

$$\begin{array}{llll} \overline{0} = \{0,1,2,3\}, & \overline{1} = \{0,4,5,6\}, & \overline{2} = \{0,9,10,11\}, & \overline{3} = \{0,7,8,12\}, \\ \overline{4} = \{1,4,8,9\}, & \overline{5} = \{1,6,7,11\}, & \overline{6} = \{1,5,10,12\}, & \overline{7} = \{3,5,8,11\}, \\ \overline{8} = \{3,4,7,10\}, & \overline{9} = \{2,4,11,12\}, & \overline{10} = \{2,6,8,10\}, & \overline{11} = \{2,5,7,9\}, \\ \overline{12} = \{3,6,9,12\}. & & & \end{array} \tag{2.2}$$

2.2. **The basic $\mathbb{P}_3$-game and M_{13}.** We now describe a "game" similar to Loyd's 15-puzzle, but played on the projective plane $\mathbb{P}_3$ rather than a square grid. Throughout, we use the self-dual labelling (2.2).

To start the game, we place counters numbered $1, \ldots, 12$ on the respective points of $\mathbb{P}_3$, leaving a hole at the point 0. A move of the game is defined as follows. Suppose that the hole is a point p and that $\ell = \{p, q, r, s\}$ is a line of $\mathbb{P}_3$. Then the move $[p, q]$ consists of moving the counter on q to p and interchanging the counters on r and s. This notation is justified because the pair $\{r, s\}$ is uniquely determined by the points p and q, by the definition of a projective plane of order 3. Moreover, the move $[p, q]$ transfers the hole from p to q, so the next move must be of the form $[q, t]$ for some t. In general, a sequence of moves can be given by specifying the path traversed by the hole:

$$[p_0,\, p_1,\, \ldots,\, p_n] \;=\; [p_{n-1}, p_n] \circ \ldots \circ [p_1, p_0]. \tag{2.3}$$

By convention, the move $[p, p]$ is trivial, so there are 12 nontrivial legal moves playable from each position of the game.

The move $[p, q]$ may be regarded as inducing the permutation $(p\ q)(r\ s) \in \mathfrak{S}_{13}$, and a move sequence such as that of (2.3) induces the permutation

$$(p_{n-1}\ p_n)(q_n\ r_n) \cdots (p_0\ p_1)(q_1\ r_1),$$

where q_i, r_i are the other two points on the line $\overline{p_{i-1}p_i}$ for each i (assuming that the sequence contains no trivial moves). Here multiplication proceeds right to left, as is usual for permutations.

Example 2.3. Consider the path $[0, 6, 12, 1, 8, 0]$. Since the points 0 and 6 are collinear with 4 and 5, the first move $[0, 6]$ induces the permutation (0 6)(4 5). The permutation induced by the entire path is

$$(0\ 8)(7\ 12)\cdot(1\ 8)(4\ 9)\cdot(1\ 12)(5\ 10)\cdot(6\ 12)(3\ 9)\cdot(0\ 6)(4\ 5) \\ = (1\ 7\ 12\ 6\ 8)(3\ 4\ 10\ 5\ 9).$$

Two paths are called *equivalent* if they induce the same permutation. We readily check that if p, q, r are collinear then the paths $[p, q, r]$ and $[p, r]$ are equivalent. It follows that every path is equivalent to a path of equal or shorter length in which no three consecutive points are collinear; we say that such a path is *nondegenerate*.

We say that a path $[p_0, \dots, p_n]$ is *closed* if $p_0 = p_n$. The set of permutations induced by closed move sequences with $p_0 = p_n = 0$ is a subgroup of the symmetric group $\mathfrak{S}_{\mathcal{P}\setminus\{0\}} = \mathfrak{S}_{12}$. We call this subgroup the *basic $\mathbb{P}_3$-game group* G_{bas}, and denote its identity element by $\mathbf{1}$.

The permutations realized by move sequences taking the hole from p to q constitute a double coset of G_{bas} in $\mathfrak{S}_{\mathcal{P}}$, namely $[0, q]\, G_{\text{bas}}\, [p, 0]$. In the case that $p = q$, this double coset is a group which we call the *q-conjugate of G_{bas}*.

We denote by M_{13} the set of all (not necessarily closed) move sequences with $p_0 = 0$. This name will be justified when we prove that G_{bas} is isomorphic to the Mathieu group M_{12}. Note that M_{13} is not a group: the moves available in a given position depend on the location of the hole, so concatenation of move sequences is not always allowed. Rather, M_{13} is a disjoint union of cosets of G_{bas} in $\mathfrak{S}_{\mathcal{P}} = \mathfrak{S}_{13}$.

2.3. **The signed $\mathbb{P}_3$-game.** We now describe the *signed $\mathbb{P}_3$-game*, an extension of the $\mathbb{P}_3$-game in which each counter has two distinguishable sides. Suppose that the hole is at $p \in \mathcal{P}$ and that $\ell = \{p, q, r, s\} \in \mathcal{L}$. The move $[p, q]$ of the signed game moves the counter on q to p and interchanges the counters on r and s, but it also flips over the counters on r and s. Now a move sequence may be regarded as inducing a signed permutation on $\mathcal{P}$ (that is, an element of the wreath product $\mathbb{Z}/2\mathbb{Z} \wr \mathfrak{S}_{\mathcal{P}}$).

Example 2.4. The path $[0, 6, 12, 1, 8, 0]$ induces the permutation

$$(0\ 8)(\underline{7}\ \underline{12})\cdot(1\ 8)(\underline{4}\ \underline{9})\cdot(1\ 12)(\underline{5}\ \underline{10})\cdot(6\ 12)(\underline{3}\ \underline{9})\cdot(0\ 6)(\underline{4}\ \underline{5}) \\ = (\underline{1}\ \underline{7}\ 12\ 6\ 8)(3\ 4\ \underline{10}\ 5\ \underline{9}).$$

Here the underlines denote flips; thus the counters flipped by the move sequence are 1, 7, 9, and 10. Ignoring all the flips is tantamount to removing all the underlines from the calculation, which recovers the unsigned permutation of Example 2.3.

Much of the terminology of the previous section (such as "closed", "degenerate", etc.) carries over to the signed game. The group of signed permutations of $\mathcal{P} \setminus \{0\}$ induced by closed move sequences is called the *signed $\mathbb{P}_3$-game group*, denoted G_{sgn}; and the set of signed permutations induced by the move sequences with $p_0 = 0$ is called $2M_{13}$.

3. The signed game, the Golay code, and the Mathieu group

In this section, we prove the main results that the basic $\mathbb{P}_3$-game group G_{bas} is isomorphic to the Mathieu group M_{12}, and that the signed game group G_{sgn} is the nontrivial double cover $2M_{12}$.

Let $\mathbb{F}_3 = \{0, 1, -1\}$ be the field of order 3, and let X be a 13-dimensional vector space over $\mathbb{F}_3$ with basis $\{x_p \mid p \in \mathcal{P}\}$. We will write elements of X in the form $v = \sum_p v_p x_p$, where $v_p \in \mathbb{F}_3$. Define a scalar product on X by

$$v \cdot w = \sum_{p \in \mathcal{P}} v_p w_p. \tag{3.1}$$

The *support* of the vector v is

$$\operatorname{Supp}(v) = \{p \in \mathcal{P} \mid v_p \neq 0\}$$

and its *weight* is

$$\operatorname{wt}(v) = |\operatorname{Supp}(v)|.$$

We will refer to vector subspaces of X as *codes*, and to their elements as *codewords*. The *minimal weight* of a code X' is

$$\operatorname{wt}_{\min}(X') = \min\{\operatorname{wt}(c) \mid c \in X',\ c \neq 0\}.$$

Let $\mathcal{C} \subset X$ be the linear span of the 13 vectors

$$h_\ell = \sum_{p \in \ell} x_p$$

where ℓ ranges over $\mathcal{L}$, and define

$$\mathcal{C}' = \{c \in \mathcal{C} \;\Big|\; \sum_p c_p = 0\},$$

a codimension-1 subcode of $\mathcal{C}$. (Note that $\mathcal{C}' \neq \mathcal{C}$ because $h_\ell \notin \mathcal{C}'$.) We will show that for each $p \in \mathcal{P}$, there is a copy $\mathcal{C}_p$ of the ternary Golay code [Conway:1999, p. 85] occurring naturally as a subcode of $\mathcal{C}$. First, we set forth some useful properties of $\mathcal{C}$ and $\mathcal{C}'$.

Proposition 3.1. *Let $c \in \mathcal{C}$. Then:*

(1) $\displaystyle\sum_{p \in \mathcal{P}} c_p^2 = \left(\sum_{p \in \mathcal{P}} c_p\right)^2$.
(2) $\operatorname{wt}(c) \equiv 0$ *or* $1 \pmod 3$.
(3) $c \in \mathcal{C}'$ *iff* $\operatorname{wt}(c) \equiv 0 \pmod 3$.
(4) *For each $\ell \in \mathcal{L}$,*
$$\sum_{p \in \mathcal{P}} c_p = \sum_{p \in \ell} c_p.$$
(5) $\mathcal{C}' = \mathcal{C}^\perp$, *the orthogonal complement of $\mathcal{C}$ with respect to the scalar product (3.1).*
(6) $\dim \mathcal{C} = 7$ *and* $\dim \mathcal{C}' = 6$.
(7) $\operatorname{wt}_{\min}(\mathcal{C}) = 4$ *and* $\operatorname{wt}_{\min}(\mathcal{C}') = 6$. *Moreover, the weight-4 codewords in $\mathcal{C}$ are precisely $\{\pm h_\ell \mid \ell \in \mathcal{L}\}$.*

Proof. (1) It suffices to show that

$$\sum_{p\in\mathcal{P}} c_p d_p = \left(\sum_{p\in\mathcal{P}} c_p\right)\left(\sum_{p\in\mathcal{P}} d_p\right) \tag{3.2}$$

for all $c, d \in \mathcal{C}$. Since this identity is bilinear in c and d, we need only consider the case $c = h_\ell$, $d = h_m$, when both sides evaluate to 1 (whether or not $\ell = m$).

(2) Since the square of each nonzero element of $\mathbb{F}_3$ is 1, we have

$$\mathrm{wt}(c) \equiv \sum_{p\in\mathcal{P}} c_p^2 \pmod 3.$$

By part (1), the right-hand side is a square in $\mathbb{F}_3$, hence either 0 or 1.

(3) This follows from the definition of $\mathcal{C}'$, together with the previous two parts.

(4) It suffices to verify the desired identity for the generators h_ℓ. Indeed, let $c = h_m$; then both sides of the identity are equal to 1 whether ℓ and m are the same or different.

(5) If $c \in \mathcal{C}'$, then the right-hand side of (3.2) is zero for every $d \in \mathcal{C}$; it follows that $\mathcal{C} \subset (\mathcal{C}')^\perp$. To prove the reverse inclusion, let $w \in (\mathcal{C}')^\perp$. If $\mathrm{Supp}(w)$ intersects some line ℓ in more than two points, then we can reduce $\mathrm{wt}(w)$ by adding h_ℓ or $-h_\ell$ to w. Repeating this process, we eventually obtain a codeword $w' \in C_0^\perp$ which is congruent to w modulo $\mathcal{C}$ (since $h_\ell \in \mathcal{C} \subset (\mathcal{C}')^\perp$) and such that $\mathrm{Supp}(w')$ intersects no line in more than two points. By Proposition 2.2, $\mathbb{P}_3$ contains no hyperovals, so $\mathrm{wt}(w') \le 4$.

Suppose that $\mathrm{wt}(w') \neq 0$. Then there is a line ℓ disjoint from $\mathrm{Supp}(w')$ and another line m intersecting $\mathrm{Supp}(w')$ in exactly one point. The vector $h_\ell - h_m$ belongs to C_0 but is not orthogonal to w, which is impossible since $\mathcal{C} \subset (\mathcal{C}')^\perp$. Hence $\mathrm{wt}(w') = 0$, $w' = 0$, and $w \in \mathcal{C}$.

(6) By part (5), $\dim \mathcal{C}' + \dim(\mathcal{C}')^\perp = 13 = 2\dim\mathcal{C} - 1$. Hence $\dim \mathcal{C}' = 6$ and $\dim \mathcal{C} = 7$.

(7) Clearly $\mathrm{wt}(h_\ell) = 4$ for every line ℓ. Let $c \in \mathcal{C}$ be a codeword of minimal nonzero weight. If $\mathrm{Supp}(c)$ meets no line of $\mathbb{P}_3$ in more than two points, then $c = 0$ by the argument of (5). In particular $\mathrm{wt}(c) \neq 1$. By part (2), $\mathrm{wt}(c) \notin \{2, 5\}$. If $\mathrm{wt}(c) \in \{3, 4\}$, then $|\mathrm{Supp}(c) \cap \ell| \ge 3$ for some line ℓ. But then the weight of c can be reduced by adding or subtracting h_ℓ. Since c is of minimal weight, this is a contradiction unless $c = \pm h_\ell$. Hence $\mathrm{wt}_{\min}(\mathcal{C}) = 4$. By part (3), we have $\mathrm{wt}_{\min}(\mathcal{C}') \ge 6$. In fact, $\mathrm{wt}_{\min}(\mathcal{C}') = 6$ because $\mathrm{wt}(h_\ell - h_m) = 6$ for $\ell \neq m$.

□

Note that $|\mathcal{C}| = 3^7 = 2187$, which is small enough that all the assertions of Proposition 3.1 could also be checked by an easily feasible but unenlightening computation.

For each $p \in \mathcal{P}$, define a subcode

$$\{c \in \mathcal{C} \mid c_p = -\sum_{q\in\mathcal{P}} c_q\},$$

and let $\mathcal{G}_p$ be the restriction of $\mathcal{C}_p$ to the coordinates $\mathcal{P} \setminus \{p\}$ (that is, the image of $\mathcal{C}_p$ modulo the subspace spanned by x_p).

Proposition 3.2. *$\mathcal{G}_p$ is isomorphic to the ternary Golay code $\mathscr{C}_{12}$ for every $p \in \mathcal{P}$.*

Proof. $\mathcal{C}_p \subsetneq \mathcal{C}$ because $h_\ell \notin \mathcal{C}_p$ for all ℓ. The kernel of the restriction map $\phi : \mathcal{C}_p \to \mathcal{G}_p$ can contain only vectors of weight ≤ 1, but $\mathrm{wt}_{\min}(\mathcal{C}_p) = 4$, so $\ker \phi = 0$. Thus ϕ is a bijection and $\dim \mathcal{G}_p = \dim \mathcal{C}_p = 6$.

For all $c \in \mathcal{C}_p$,

$$\begin{aligned} \mathrm{wt}(\phi(c)) &\equiv \sum_{q \neq p} c_q^2 \pmod 3 \\ &= -c_p^2 + \sum_{q \in \mathcal{P}} c_q^2 \;=\; -c_p^2 + \left(\sum_{q \in \mathcal{P}} c_q\right)^2 \;\equiv\; 0 \pmod 3; \end{aligned}$$

and for all $c, d \in \mathcal{C}_p$,

$$\begin{aligned} \phi(c) \cdot \phi(d) &= \sum_{q \neq p} c_q d_q \;=\; -c_p d_p + \sum_{q \in \mathcal{P}} c_q d_q \\ &= -c_p d_p + \left(\sum_{q \in \mathcal{P}} c_q\right)\left(\sum_{q \in \mathcal{P}} d_q\right) \;=\; 0 \end{aligned}$$

by (3.2). Hence $\mathcal{G}_p \subseteq \mathcal{G}_p^\perp$, whence G_p is self-dual since it has dimension $6 = 12/2$. Moreover, $\mathrm{wt}_{\min}(\mathcal{G}_p) \ge \mathrm{wt}_{\min}(\mathcal{C}) = 4$ (which implies that $\mathrm{wt}_{\min}(\mathcal{G}_p) \ge 6$ because $\mathcal{G}_p \subseteq \mathcal{G}_p^\perp$). Therefore $\mathcal{G}_p \cong \mathscr{C}_{12}$ [Conway:1999, p. 436]. □

Suppose $\ell = \{p, q, r, s\}$. Let the move $[p, q]$ of the signed $\mathbb{P}_3$-game act linearly on X by $[p, q] \cdot w = w'$, where

$$\begin{aligned} w'_p &= w_q, & w'_r &= -w_s, & w'_t &= w_t \quad \text{for } t \notin \ell, \\ w'_q &= -w_p - w_q, & w'_s &= -w_r. \end{aligned} \tag{3.3}$$

Proposition 3.3. *For all $p, q \in \mathcal{P}$, $[p, q] \cdot \mathcal{C}_p \;=\; \mathcal{C}_q$.*

Proof. Let $\ell = \{p, q, r, s\}$ as above. Since the linear transformation (3.3) is invertible, it suffices to prove the inclusion $[p, q] \cdot \mathcal{C}_p \subset \mathcal{C}_q$. Let $c \in \mathcal{C}_p$ and $d = [p, q] \cdot c$. By part (4) of Proposition 3.1,

$$\begin{aligned} c_p \;=\; -\sum_{t \in \mathcal{P}} c_t \;&=\; -\sum_{t \in \ell} c_t \\ &= -c_p - c_q - c_r - c_s \end{aligned}$$

which implies that $c_p = c_q + c_r + c_s$, since we are working over $\mathbb{F}_3$. Hence

$$\begin{aligned} c - d &= \sum_{t \in \ell} (c_t - d_t) x_t \\ &= (c_p - c_q)(x_p + x_q) + (c_r + c_s)(x_r + x_s) \\ &= (c_p - c_q) h_\ell. \end{aligned}$$

So $c - d \in \mathcal{C}$ and $d \in \mathcal{C}$. Moreover,

$$\begin{aligned} \sum_{t \in \mathcal{P}} d_t \;=\; \sum_{t \in \ell} d_t \;&=\; d_p + d_q + d_r + d_s \\ &= -c_p - c_s - c_r \\ &= c_p + c_q \;=\; -d_q. \end{aligned}$$

Therefore $d \in \mathcal{C}_q$. □

A move sequence $[p_0, \dots, p_n]$ acts on X by the composition of the linear transformations (3.3) associated with the moves $[p_i, p_{i+1}]$. It follows from Proposition 3.3 that the linear transformation associated with $[p_0, \dots, p_n]$ restricts to an isomorphism of $\mathcal{C}_0$ with $\mathcal{C}_{p_n}$. In particular, if $p_0 = p_n = 0$, then σ induces an automorphism of the code $\mathcal{C}_0$. Accordingly, G_{sgn} is naturally isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{G}_0)$.

Proposition 3.4. *G_{bas} is isomorphic to a subgroup of M_{12}.*

Proof. The center Z of $\mathrm{Aut}(\mathcal{G}_0)$ has order two (it contains the identity map and its negative), and $\mathrm{Aut}(\mathcal{G}_0)/Z \cong M_{12}$ (see [Conway:1999, p. 85]). On the other hand, the permutation $-\mathbf{1}$ corresponding to the closed path

$$[0, 10, 7, 0, 4, 1, 2, 4, 3, 5, 6, 3, 0] \tag{3.4}$$

flips each of the 12 counters without changing its location. Clearly $-\mathbf{1}$ is central and has order 2. Hence $G_{\mathrm{sgn}}/\{\mathbf{1}, -\mathbf{1}\}$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{G}_0)/Z \cong M_{12}$. On the other hand, $G_{\mathrm{sgn}}/\{\mathbf{1}, -\mathbf{1}\} = G_{\mathrm{bas}}$, because taking the quotient by $-\mathbf{1}$ is equivalent to ignoring flips. □

We see now that a permutation σ in M_{12} (resp. M_{13}) has two *lifts* σ_1, σ_2 in $2M_{12}$ (resp. $2M_{13}$), both of which are equivalent to σ as unsigned permutations and such that $\sigma_1^{-1} \circ \sigma_2 = -\mathbf{1}$.

To establish the reverse inclusion, we used a computer program (in C) to generate a list of all permutations arising from closed move sequences.[1] Rather than reproduce the entire list here, we use the presentation of M_{12} as a subgroup of the symmetric group $\mathfrak{S}_{12}$ with generators given in cycle notation by

$$\begin{aligned} \alpha &= (1\ 6\ 4\ 2\ 11\ 3\ 8\ 9\ 10\ 7\ 5), \\ \gamma &= (1\ 12)(2\ 9)(3\ 4)(5\ 6)(7\ 8)(10\ 11), \\ \delta &= (4\ 5)(2\ 11)(3\ 7)(8\ 9). \end{aligned} \tag{3.5}$$

(see [Conway:1999, p. 273]; we have changed the labelling of the points to conform with (2.2)). Indeed, the move sequences

$$[0, 11, 7, 9, 8, 3, 0], \qquad [0, 12, 1, 9, 0, 3, 8, 4, 0], \qquad [0, 1, 7, 0, 3, 6, 0, 1, 7, 0]$$

induce the permutations α, γ and δ respectively. Combining this with Proposition 3.4 and the known identification of $2M_{12}$ with $\mathrm{Aut}(\mathcal{G}_0)$ [Conway:1985], we have proved:

Theorem 3.5.

(1) *The basic $\mathbb{P}_3$-game group G_{bas} is isomorphic to the Mathieu group M_{12}, acting sharply quintuply transitively on $\mathcal{P} \setminus \{0\}$.*
(2) *The signed game group G_{sgn} is isomorphic with $2M_{12}$, with Z the 2-element normal subgroup and $G_{\mathrm{sgn}}/Z \cong M_{12}$.*

4. The dualized game

We can extend the $\mathbb{P}_3$-game in another way by placing a second set of counters on the lines of $\mathbb{P}_3$. This version of the game provides a second proof that the game group is M_{12}, realized as the group of automorphisms of a 12×12 *Hadamard matrix* (that is, an orthogonal matrix all of whose entries are ± 1). In addition,

[1] The source code appears in [Martin:1996], and is now online at `http://www.math.harvard.edu/~elkies/M13` .

interchanging the roles of points and lines gives a concrete interpretation of the outer automorphisms of M_{12}.

We began the basic $\mathbb{P}_3$-game by placing 12 numbered counters on the points $\mathcal{P} \setminus \{0\}$. In the dualized game, we place in addition 12 numbered "line-counters" on the lines $\mathcal{L} \setminus \{\overline{0}\}$. The move sequences of the dualized game are defined similarly to those of the basic game, with the proviso that the point-hole must always lie on the line-hole. Specifically, suppose that the point-hole and line-hole are located at p and ℓ respectively, with $\mathcal{L}(p) = \{\ell, m, n, k\}$ and $\ell = \{p, q, r, s\}$. The point-move $[p, q]$ is defined as in the basic game; dually, the line-move $[\ell, m]$ consists of moving the line-counter on m to the hole at ℓ and interchanging the line-counters on n and k. Thus a move sequence has the general form

$$([p_0, \ldots, p_n],\ [\ell_0, \ldots, \ell_n]) \ = \ [\ell_{n-1}, \ell_n] \circ [p_{n-1}, p_n] \circ \cdots \circ [\ell_0, \ell_1] \circ [p_0, p_1] \quad (4.1)$$

subject to the conditions $p_i,\ p_{i+1} \in \ell_i$ and $\ell_i,\ \ell_{i+1} \in \mathcal{L}(p_{i+1})$ for all i. Each move sequence induces a pair of permutations $\sigma = (\sigma_{\mathcal{P}}, \sigma_{\mathcal{L}})$, where $\sigma_{\mathcal{P}}$ acts on the point-counters and $\sigma_{\mathcal{L}}$ acts on the line-counters.

It is easy to verify that for every move sequence $([p_0, \ldots, p_n],\ [\ell_0, \ldots, \ell_n])$ of the dualized game, the point-path $[p_0, \ldots, p_n]$ is nondegenerate if and only if the line-path $[\ell_0, \ldots, \ell_n]$ is. As before, every move sequence is equivalent to one in which both paths are nondegenerate.

A move sequence of the dualized game is called *closed* if it returns both the point-hole and the line-hole to their initial locations. The group of permutations induced by closed moves is called the *dualized* $\mathbb{P}_3$*-game group*, written G_{dual}. In fact, we shall show that $G_{\mathrm{dual}} \cong G_{\mathrm{bas}}$, and indeed that the point-permutation of an element of G_{dual} determines the line-permutation uniquely and vice versa.

Example 4.1. As in Examples 2.3 and 2.4), consider the path $[0, 6, 12, 1, 8, 0]$. For this to be the point-path of a closed move sequence in the dualized game, the corresponding line-path can only be

$$\left[\overline{0\ 6},\ \ \overline{6\ 12},\ \ \overline{12\ 1},\ \ \overline{1\ 8},\ \ \overline{8\ 0}\right] \ = \ \left[\overline{0}, \overline{1}, \overline{12}, \overline{6}, \overline{4}\right].$$

The moves of the dualized game may be interpreted as automorphisms of a 12×12 Hadamard matrix H. An *automorphism* of H may be defined as a pair (σ, τ) of signed permutation matrices such that $\sigma H \tau = H$. The group $\mathrm{Aut}(H)$ of all automorphisms is isomorphic to $2M_{12}$ [Conway:1985, p. 32]. In what follows, we construct an isomorphism of G_{dual} with $\mathrm{Aut}(H)$.

Define a modified incidence matrix $E = (e_{ij})$ for $\mathbb{P}_3$, with rows i indexed by $\mathcal{P}$ and columns j indexed by $\mathcal{L}$, by

$$e_{ij} = \begin{cases} -1 & i \in j, \\ +1 & i \notin j. \end{cases}$$

Labelling the points and lines of $\mathbb{P}_3$ self-dually, as in (2.2), makes E into a symmetric matrix. Each row of E contains four -1's and nine $+1$'s, and each pair of distinct rows agree in exactly seven columns, so the scalar product $E_r \cdot E_s$ of two rows of E is

$$E_r \cdot E_s \ = \ \sum_j e_{rj} e_{sj} \ = \ \begin{cases} 13 & r = s, \\ 1 & r \neq s. \end{cases} \quad (4.2)$$

Next, for all pairs p, ℓ with $p \in \ell$, define a 12×12 matrix $H^{p,\ell}$, with rows indexed by $\mathcal{P} \setminus \{p\}$ and columns indexed by $\mathcal{L} \setminus \{\ell\}$, by

$$(H^{p,\ell})_{ij} \;=\; \begin{cases} -e_{ij} & i \in \ell \text{ and } j \in \mathcal{L}(p) \\ e_{ij} & \text{otherwise.} \end{cases} \tag{4.3}$$

Proposition 4.2. *Let $p \in \mathcal{P}$ and $\ell \in \mathcal{L}(p)$. Then $H = H^{p,\ell}$ is a Hadamard matrix.*

Proof. H can be made symmetric by choosing a self-dual labelling in which p and ℓ have the same label. Thus, to prove the proposition, it is enough to show that for each pair of distinct points $r, s \in \mathcal{P} \setminus \{p\}$, the scalar product $H_r \cdot H_s$ of the corresponding rows of H is zero.

If $r \notin \ell$ and $s \notin \ell$, then $e_{r\ell} = e_{s\ell} = 1$, so

$$H_r \cdot H_s \;=\; \sum_{j \in \mathcal{L} \setminus \{\ell\}} e_{rj} e_{sj} \;=\; -e_{rl} e_{sl} \;+\; \sum_{j \in \mathcal{L}} e_{rj} e_{sj} \;=\; -1 + E_r \cdot E_s \;=\; 0.$$

If $r \in \ell$ and $s \in \ell$, then $e_{r\ell} = e_{s\ell} = -1$, so

$$H_r \cdot H_s \;=\; \sum_{j \in \mathcal{L}(p) \setminus \{\ell\}} (-e_{rj})(-e_{sj}) \;+\; \sum_{j \in \mathcal{L} \setminus \mathcal{L}(p)} e_{rj} e_{sj} \;=\; \sum_{j \in \mathcal{L} \setminus \{\ell\}} e_{rj} e_{sj} \;=\; 0$$

by the previous case. Finally, suppose that $r \in \ell$ and $s \notin \ell$. Then $e_{r\ell} = -1$ and $e_{s\ell} = 1$, so

$$H_r \cdot H_s \;=\; -\sum_{j \in \mathcal{L}(p) \setminus \{\ell\}} e_{rj} e_{sj} \;+\; \sum_{j \in \mathcal{L} \setminus \mathcal{L}(p)} e_{rj} e_{sj}.$$

Moreover,

$$1 \;=\; \sum_{j \in \mathcal{L}} e_{rj} e_{sj} \;=\; -1 + \sum_{j \in \mathcal{L} \setminus \mathcal{L}(p)} e_{rj} e_{sj} \;+\; \sum_{j \in \mathcal{L}(p) \setminus \{\ell\}} e_{rj} e_{sj}.$$

by (4.2). Combining these two observations, we obtain

$$H_r \cdot H_s \;=\; 2 \left(1 - \sum_{j \in \mathcal{L}(p) \setminus \{\ell\}} e_{rj} e_{sj} \right). \tag{4.4}$$

Since $\overline{pr} = \ell$, the three e_{rj}'s in the right-hand side of (4.4) all equal $+1$. On the other hand, $\overline{ps} \neq \ell$, so $\overline{ps}$ is one of the other lines in $\mathcal{L}(p)$. Thus one of the three e_{sj}'s is -1 and the other two are $+1$. Therefore the expression in (4.4) vanishes. □

We now associate a signed permutation matrix with each move sequence of the dualized game. For $p \in \mathcal{P}$ and $\ell = \{p, q, r, s\} \in \mathcal{L}(p)$, let $B = (b_{ij})$ be a 12×12 matrix, with rows indexed by $\mathcal{P} \setminus \{p\}$ and columns indexed by $\mathcal{L} \setminus \{\ell\}$. The point-move $[p, q]$ acts on B, producing a matrix $[p, q] \cdot B$ with rows indexed by $\mathcal{P} \setminus \{q\}$ and columns indexed by $\mathcal{L} \setminus \{\ell\}$, whose (i, j) entry is

$$([p, q] \cdot B)_{ij} \;=\; \begin{cases} b_{qj} & i = p \\ -b_{rj} & i = s \\ -b_{sj} & i = r \\ b_{ij} & \text{otherwise.} \end{cases} \tag{4.5}$$

The line-move $[\ell, m]$ acts on the columns of B in a similar way, producing a matrix with rows indexed by $\mathcal{P} \setminus \{p\}$ and columns indexed by $\mathcal{L} \setminus \{m\}$. More generally, we may associate a signed permutation matrix with each move sequence of the dual

game by composing those corresponding to its constituent moves. Note that the actions of point- and line-moves commute.

Proposition 4.3. *Let $\sigma = (\sigma_{\mathcal{P}}, \sigma_{\mathcal{L}})$ be a move sequence of the dualized game, with the point-hole initially at $p \in \mathcal{P}$ and the line-hole initially at $\ell \in \mathcal{L}(p)$. Let $H^{p,\ell}$ be the Hadamard matrix defined in* (4.3)*. Then $\sigma(H^{p,\ell}) = H^{\sigma(p),\sigma(\ell)}$.*

Proof. It is sufficient to consider the case that σ is a single point-move. The proof for line-moves is identical, and the general case will then follow by composition. Suppose therefore that $\ell = \{p, q, r, s\}$ and $\sigma = [p, q]$. The definition (4.3) may be rewritten as

$$(H^{p,\ell})_{ij} \;=\; \begin{cases} -e_{ij} & i \in \{q,r,s\} \quad \text{and} \quad j \in \mathcal{L}(p) \setminus \{\ell\} \\ +e_{ij} & i \in \mathcal{P} \setminus \ell \quad \text{and} \quad j \in \mathcal{L} \setminus \mathcal{L}(p), \end{cases}$$

so that

$$(\sigma(H^{p,\ell}))_{ij} \;=\; \begin{cases} (H^{p,\ell})_{qj} & i = p \\ -(H^{p,\ell})_{sj} & i = r \\ -(H^{p,\ell})_{rj} & i = s \\ (H^{p,\ell})_{ij} & \text{otherwise,} \end{cases}$$

and

$$(H^{q,\ell})_{ij} \;=\; \begin{cases} -e_{ij} & i \in \ell \text{ and } j \in \mathcal{L}(q) \\ +e_{ij} & \text{otherwise.} \end{cases}$$

We will show that $(\sigma(H^{p,\ell}))_{ij} = (H^{q,\ell})_{ij}$ for all i, j. First, if $i \notin \ell$, then

$$(\sigma(H^{p,\ell}))_{ij} \;=\; (H^{p,\ell})_{ij} \;=\; e_{ij} \;=\; (H^{q,\ell})_{ij}.$$

Second, suppose that $i = p$. In this case

$$\begin{aligned} (\sigma(H^{p,\ell}))_{pj} \;=\; (H^{p,\ell})_{qj} \quad &= \quad \begin{cases} -e_{qj} & j \in \mathcal{L} \setminus \mathcal{L}(p) \\ +e_{qj} & \text{otherwise} \end{cases} \\ &= \quad \begin{cases} -1 & j \in \mathcal{L}(p) \cup \mathcal{L}(q) \setminus \{\ell\} \\ +1 & \text{otherwise} \end{cases} \\ &= \quad \begin{cases} -e_{pj} & j \in \mathcal{L}(q) \setminus \{\ell\} \\ +e_{pj} & \text{otherwise} \end{cases} \\ &= \quad (H^{q,\ell})_{pj}. \end{aligned}$$

Finally, suppose that $i = r$ (the case $i = s$ is analogous). Then

$$\begin{aligned} (\sigma(H^{p,\ell}))_{rj} \;=\; -(H^{p,\ell})_{sj} \quad &= \quad \begin{cases} +e_{sj} & j \in \mathcal{L}(p) \setminus \{\ell\} \\ -e_{sj} & \text{otherwise} \end{cases} \\ &= \quad \begin{cases} +1 & j \in \mathcal{L}(p) \cup \mathcal{L}(s) \setminus \{\ell\} \\ -1 & j \in \mathcal{L}(q) \cup \mathcal{L}(r) \setminus \{\ell\} \end{cases} \\ &= \quad \begin{cases} -e_{rj} & j \in \mathcal{L}(q) \setminus \{\ell\} \\ +e_{rj} & \text{otherwise} \end{cases} \\ &= \quad (H^{q,\ell})_{rj}. \end{aligned}$$

□

Corollary 4.4. $G_{\text{dual}} \cong G_{\text{bas}}$ ($\cong M_{12}$).

Proof. Proposition 4.3 implies that for each closed move σ of the dualized game, the pair of (unsigned) permutations $(\sigma_{\mathcal{P}}, \sigma_{\mathcal{L}})$ is an automorphism of the Hadamard matrix $H = H^{p,\ell}$. That is, we have an injective group homomorphism from G_{dual} to $\text{Aut}(H)/\{\pm\mathbf{1}\} \cong M_{12}$. On the other hand, the permutations (3.5) generate a subgroup of G_{dual} that is isomorphic to M_{12}. □

Denote by $\text{Aut}(M_{12})$ the group of automorphisms of M_{12}, and by $\text{Inn}(M_{12})$ the normal subgroup of inner automorphisms (that is, automorphisms given by conjugation). Then $\text{Inn}(M_{12}) \cong M_{12}$ since M_{12} is simple and nonabelian, and the quotient $\text{Aut}(M_{12})/\text{Inn}(M_{12})$ has order two [Conway:1985, p. 31]. The dualized game allows us to describe an outer automorphism (and thus the full automorphism group) of M_{12} explicitly. Consider the map

$$\begin{array}{rccc} \theta: & G_{\text{dual}} & \to & G_{\text{dual}} \\ & (\sigma_P, \sigma_L) & \mapsto & (\sigma_L, \sigma_P). \end{array} \tag{4.6}$$

Proposition 4.5. *The map θ is an outer automorphism of $G_{\text{dual}} \cong M_{12}$.*

Proof. The map θ respects concatenation of paths, so it is a group homomorphism $G_{\text{dual}} \to G_{\text{dual}}$. It is clearly surjective, hence an automorphism. It remains only to show that θ is not conjugation by any element of G_{dual}.

Consider the point-paths $\pi_1 = [0,1,4,0]$, $\pi_2 = [0,2,10,0]$ and $\pi_3 = [0,3,12,0]$, whose induced permutations are respectively

$$\alpha_1 = (1\,4)(2\,3)(5\,6)(8\,9), \quad \alpha_2 = (1\,3)(2\,10)(6\,8)(9\,11), \quad \alpha_3 = (1\,2)(3\,12)(6\,9)(7\,8).$$

By the labelling (2.2), for each i, the line-path corresponding to π_i is its reverse, so $\theta(\alpha_i) = \alpha_i^{-1} = \alpha_i$ (because each α_i is an involution). Therefore, if θ is conjugation by some permutation σ, then σ must commute with each α_i. A Maple computation (which is not hard to check by hand) reveals that the intersection of the $\mathfrak{S}_{12}$-centralizers of the α_i's contains exactly one non-identity element, namely

$$\sigma = (1\,6)(2\,9)(3\,8)(4\,5)(7\,12)(10\,11).$$

(In fact, this permutation commutes with every fixed point of the automorphism θ.) Now, consider the point-path $[0,1,5,0]$, whose associated line-path is $[0,6,1,0]$. The induced point- and line-permutations are respectively $(1\,5)(2\,3)(4\,6)(10\,12)$ and $(1\,6)(2\,3)(4\,5)(7\,11)$. Then θ interchanges these two permutations; however, they are not conjugates under σ. It follows that θ is not conjugation by any element of $\mathfrak{S}_{12}$, so *a fortiori* not by any element of M_{12}; that is, θ is an outer automorphism. □

Corollary 4.6. $\langle G_{\text{dual}}, \theta \rangle = \text{Aut}(G_{\text{dual}}) = \text{Aut}(M_{12})$.

5. M_{13} and sextuple transitivity

5.1. **Multiply transitive groups.** We recall some basic terminology. Let G be a (finite) group acting on a (finite) set X; that is, there is a group homomorphism from G to $\mathfrak{S}_X$, the group of permutations of X. The action is called *faithful* if this homomorphism is one-to-one and *transitive* if the action has a single orbit. More generally, the action is *k-transitive* if $|X| \geq k$ and for any two k-tuples of distinct elements of X, say $\mathbf{p} = (p_1, \ldots, p_k)$ and $\mathbf{q} = (q_1, \ldots, q_k)$, there exists $g \in G$ such that $g \cdot p_i = q_i$ for all i. If the element g is unique, then the action is *sharply*

k-transitive. Note that a group G with a faithful, sharply k-transitive action on an r-set must have cardinality $r!/(r-k)!$.

Groups with highly transitive actions are quite unusual: by the classification of finite simple groups, the only groups with a sharply quintuply transitive action are M_{12}, $\mathfrak{S}_5$, $\mathfrak{S}_6$ and $\mathfrak{A}_7$, and there are no sextuply transitive groups other than $\mathfrak{S}_7$ and $\mathfrak{A}_8$. In particular—and this does not require the Classification Theorem—it is not possible to continue Mathieu's construction of M_{11} and M_{12} to a transitive subgroup of $\mathfrak{S}_{13}$ other than $\mathfrak{A}_{13}$ and $\mathfrak{S}_{13}$ itself. Yet we have obtained the pseudogroup M_{13} by a method similar to this construction. M_{12}, realized as the game group G_{bas}, acts faithfully and sharply 5-transitively on the 12-element set $\mathcal{P} \setminus \{0\}$. Meanwhile, M_{13} "acts" on the 13-element set $\mathcal{P}$, and $|M_{13}| = 13|M_{12}|$, just what the order of a sharply sextuply transitive group ought to be.

We are thus led to consider the question: Is the "action" of M_{13} on $\mathcal{P}$ sextuply transitive? That is, given two sextuples $\mathbf{p} = (p_1, \ldots, p_6)$ and $\mathbf{q} = (q_1, \ldots, q_6)$ of points of $\mathbb{P}_3$, does there exist some $\sigma \in M_{13}$ such that $\sigma(p_i) = q_i$ for all i? (Here and from now on, "sextuple" means "ordered sextuple of distinct elements". In addition, we wish to include the possibility that $0 \in \mathbf{p}$, so "counter" really means "counter or hole".) Since M_{13} is not a group, there are actually two distinct questions:

(1) Fix a sextuple $\mathbf{p}$ of counters. Is it true that for all sextuples $\mathbf{q}$ of points of $\mathbb{P}_3$, there exists some $\sigma \in M_{13}$ such that $\sigma(\mathbf{p}) = \mathbf{q}$? If so, we call $\mathbf{p}$ a *universal donor*.
(2) Fix a sextuple $\mathbf{q}$ of points of $\mathbb{P}_3$. Is it true that for all sextuples $\mathbf{p}$ of counters, there exists some $\sigma \in M_{13}$ such that $\sigma(\mathbf{p}) = \mathbf{q}$? If so, we call $\mathbf{p}$ a *universal recipient*.

We will examine the questions separately. In each case, our computational data was invaluable as a source of educated guesses about sextuple transitivity. We start by making an elementary observation which will be quite useful in both cases.

Lemma 5.1. *Let $\mathbf{p}$ be a sextuple of counters. Then $\mathbf{p}$ is a universal donor if and only if, for all $\sigma, \tau \in M_{13}$ with $\sigma \neq \tau$, we have $\sigma(\mathbf{p}) \neq \tau(\mathbf{p})$. Similarly, if $\mathbf{q}$ is a sextuple of points, it is a universal recipient if and only if $\sigma \neq \tau$ implies $\sigma^{-1}(\mathbf{q}) \neq \sigma^{-1}(\mathbf{q})$.*

Proof. This follows from the pigeonhole principle, together with the observation that $|M_{13}|$ equals $13!/7!$, the number of sextuples of points in $\mathbb{P}_3$. □

5.2. **Sextuple transitivity on counters.** We consider the question of when a sextuple $\mathbf{p}$ of counters is a universal donor. Note that the property is invariant under permuting the order of the p_i. Thus, for ease of notation, we frequently treat $\mathbf{p}$ as a set: for instance, we write $\mathbf{p} \cap \ell$ rather than $\{p_i \mid 1 \leq i \leq 6\} \cap \ell$.

Theorem 5.2. *A sextuple of counters $\mathbf{p} = (p_1, \ldots, p_6)$ is a universal donor if and only if $p_i = 0$ for some i.*

Proof. Suppose first that $p_i = 0$ for some i. Let $\mathbf{q} = (q_1, \ldots, q_6)$ be an arbitrary sextuple of points. Note that the move $[0, q_i]$ takes the hole from p_i to q_i. The q_i-conjugate of G_{bas} acts quintuply transitively on $\mathcal{P} \setminus \{q_i\}$, hence contains a permutation σ such that

$$\big(\sigma \circ [0, q_i]\big)(p_j) = q_j$$

for all $j \neq i$. That is, $\sigma \circ [0, q_i]$ is the desired element of M_{13} taking $\mathbf{p}$ to $\mathbf{q}$.

Now suppose that $0 \notin \mathbf{p}$. The set $\mathcal{P} - \mathbf{p} - \{0\}$ has cardinality six. Since $\mathbb{P}_3$ has no hyperhyperovals (as discussed in Section 2.1), there is some line ℓ that meets $\mathcal{P} - \mathbf{p} - \{0\}$ in at least three points; that is, the set $A = (\mathbf{p} \cup \{0\}) \cap \ell$ has at most one element. We consider three cases; in each case, we will exhibit two moves $\sigma, \tau \in M_{13}$ that act equally on the counters of $\mathbf{p}$; by Lemma 5.1, such a pair will suffice to show that $\mathbf{p}$ is not a universal donor.
Case 1: $A = \{0\}$. Then $\ell \cap \mathbf{p} = \emptyset$, so $[0, q]$ fixes each counter in $\mathbf{p}$ for any point $q \in \ell$ other than 0. Thus we may take $\sigma = \mathbf{1}$ and $\tau = [0, q]$.
Case 2: $A = \{p_i\}$ *for some* i. Let q be any point on ℓ other than p_i. Playing the move $[0, p_i]$ results in a position in which ℓ contains no counters of $\mathbf{p}$; therefore, we may take $\sigma = [0, p_i]$ and $\tau = [0, p_i, q]$.
Case 3: $A = \emptyset$. Let q, r be distinct points on ℓ. Similarly to Case 2, we may take $\sigma = [0, q]$ and $\tau = [0, q, r]$. □

5.3. **Sextuple transitivity on points.** We now consider the question of when a sextuple $\mathbf{q}$ of points is a universal recipient. As before, we shall make no notational distinction between the ordered sextuple $\mathbf{q}$ and its underlying set.

Theorem 5.3. *A sextuple of points* $\mathbf{q} = (q_1, \ldots, q_6)$ *is a universal recipient if and only if it contains some line of* $\mathbb{P}_3$.

Proof. Suppose that $\mathbf{q}$ contains a line ℓ. Let $\mathbf{p}$ be a sextuple of counters; our goal is to find $\sigma \in M_{13}$ taking $\mathbf{p}$ to $\mathbf{q}$. If $0 \in \mathbf{p}$, then $\mathbf{p}$ is a universal donor by Theorem 5.2 so we are done. Suppose now that $0 \notin \mathbf{p}$. Without loss of generality we may suppose that $\ell = \{q_1, q_2, q_3, q_4\}$, and that the line $m = \overline{q_5 q_6}$ meets ℓ at q_1. Let x be the fourth point on this line.

By quintuple transitivity, the q_1-conjugate of G_{bas} contains a move τ such that $\tau(p_i) = q_i$ for $2 \le i \le 6$. Consider the move $\upsilon = \tau \circ [0, q_1]$; note that $\upsilon(p_1) \notin \mathbf{q}$. If $\upsilon(p_1) \neq x$, then

$$\sigma \;=\; [q_1, \upsilon(p_1)] \;\circ\; \tau \;\circ\; [0, q_1]$$

is the desired move of M_{13} taking $\mathbf{p}$ to $\mathbf{q}$.

On the other hand, suppose $\upsilon(p_1) = x$. The move sequence $[q_1, q_2, x, q_3, q_4, x]$ induces the permutation

$$\rho \;=\; (r_2\ s_2)(r_3\ s_3)(r_4\ s_4)(q_1\ x),$$

where $\overline{x q_i} = \{x, q_i, r_i, s_i\}$ for $i = 2, 3, 4$. Hence the move

$$\sigma \;=\; \rho \;\circ\; \upsilon \;\in\; M_{13}$$

takes p_i to q_i for all i as desired.

For the "only if" direction of the theorem, suppose that $\mathbf{q}$ does not contain any line. We will show that there are two distinct elements of M_{13} which carry the same ordered sextuple of counters to the points q_i. It will follow by Lemma 5.1 that $\mathbf{q}$ is not a universal recipient.

If $\ell \cap \mathbf{q} = \emptyset$ for some line ℓ, then our task is easy. Let $p_1, p_2 \in \ell$. Then $[0, p_2]$ and $[p_1, p_2] \circ [0, p_1]$ are elements of M_{13} carrying the same set of counters to $\mathbf{q}$. By Lemma 5.1, $\mathbf{q}$ is not a universal recipient.

The more difficult case is when $\mathbf{q}$ meets every line, but does not contain any line. Since $\mathbb{P}_3$ has no hyperhyperovals, we may assume that q_1, q_2, q_5 lie on a common line ℓ (the reason for this apparently strange choice will be clear momentarily). Let y be the fourth point on ℓ. Then $y \notin \mathbf{q}$, and for $\mathbf{q}$ to meet every line, each of the

points q_3, q_4, q_6 must lie on a different line in $\mathcal{L}(y) \setminus \{\ell\}$. Thus each of the lines $\overline{q_3q_6}$, $\overline{q_4q_6}$, $\overline{q_3q_4}$ meets ℓ in a point other than y. Without loss of generality we may assume that

$$q_1 \in \overline{q_3q_6}, \qquad q_2 \in \overline{q_4q_6}, \qquad q_5 \in \overline{q_3q_4}.$$

In particular, the points q_1, q_2, q_3, q_4 form an oval. Thus we may adopt the labelling (2.1), with

$$q_5 = \overline{q_1q_2} \cap \overline{q_3q_4} = r_1, \qquad q_6 = \overline{q_1q_3} \cap \overline{q_2q_4} = r_2, \qquad y = s_{12}.$$

If $s_{12} = 0$, then the paths $[s_{12}, r_2, s_{23}]$ and $[s_{12}, r_3, r_1, s_{14}]$ induce the permutations

$$\sigma = (s_{12}\ s_{23}\ r_2)(r_3\ s_{34})(r_1\ s_{14}),$$
$$\tau = (s_{12}\ s_{14}\ r_1\ r_3)(r_2\ s_{34}\ s_{23})(s_{13}\ s_{24})$$

respectively. Both of these elements of M_{13} fix q_1, q_2, q_3, q_4, and move the counters originally located at s_{14}, s_{23} to $r_1 = q_5$ and $r_2 = q_6$ respectively. Therefore, by Lemma 5.1, $\mathbf{q}$ is not a universal recipient. On the other hand, if $s_{12} \neq 0$, then we need only preface the moves σ, τ given above by moving the hole to s_{12}. That is, the moves $[0, s_{12}, r_2, s_{23}]$ and $[0, s_{12}, r_3, r_1, s_{14}]$ move the same ordered sextuple of counters to the points $\mathbf{q}$. □

6. Metric properties

6.1. **The basic game.** Let G be a group generated by a finite set X. The *Cayley graph* of G with respect to X is the graph whose vertices are the elements of G, with g, g' connected by an edge if $g = xg'$ for some $x \in X$. We define the Cayley graph Γ of M_{13} analogously: the vertices are the 13!/7! positions of the basic game, and two positions are connected by an edge if one may be obtained from the other by a single move $[p, q]$.

We may use the Cayley graph to define a metric on M_{13}, as follows: $d(\sigma, \tau)$ is the length of the shortest path in Γ with endpoints σ and τ, that is, the minimal number of moves needed to go from σ to τ. Note that no two elements of M_{12} are adjacent in Γ. Indeed, $d(\sigma, \tau) \geq 3$ for $\sigma \neq \tau \in M_{12}$, because a two-move path returning the hole to the starting position must be of the form $[p, q] \circ [q, p] = \mathbf{1}$. Also, a path from σ to τ with length exactly $d(\sigma, \tau)$ must be nondegenerate. The *depth* of σ is defined as $d(\sigma) = d(\sigma, \mathbf{1})$. We also define

$$\begin{aligned} [M_{12}]_k &= \#\{\sigma \in M_{12} \mid d(\sigma) = k\}, \\ [M_{13}]_k &= \#\{\sigma \in M_{13} \mid d(\sigma) = k\}. \end{aligned} \tag{6.1}$$

We can find these numbers from the computer-generated table of move sequences.

Proposition 6.1. *The depth distributions for M_{12} and M_{13} are given by the following table:*

k	0	1	2	3	4	5	6	7	8	9
$[M_{12}]_k$	1	0	0	54	540	5184	25173	55044	9036	8
$[M_{13}]_k$	1	12	108	918	7344	57852	344925	733500	90852	8

We can explain some of the "shallower" numbers without resorting to computation. The unique element at depth 0 is obviously the identity. There are no moves in M_{12} at depths 1 or 2 because there are no nondegenerate closed paths having those lengths.

Let $[0, p, q, 0]$ be a nondegenerate closed path of length 3. For nondegeneracy, we must have $p \neq 0$ and $q \notin \overline{0p}$, so there are $12 \cdot 9 = 108$ such paths. The permutation induced by each path has cycle-shape 2^4 (that is, it is a quadruple transposition). This permutation has order 2, so the path $[0, q, p, 0]$ is equivalent. This is the reason that $[M_{12}]_3 = 108/2 = 54$.

Let $[0, p, q, r, 0]$ be a nondegenerate closed path of length 4. For nondegeneracy, we must have $p \neq 0$, $q \notin \overline{0p}$, and $r \notin \overline{pq} \cup \overline{q0}$, so there are $12 \cdot 9 \cdot 6 = 648$ such paths. If $\{0, p, r\}$ are collinear, then the cycle-shape of the induced permutation is 2^4; otherwise it is 3^3. In the first case, the path $[0, r, q, p, 0]$ is equivalent. There are 216 paths with $\{0, p, r\}$ collinear, so 108 of them are redundant. Since $648 - 108 = 540 = [M_{12}]_4$, there are no other equivalences among paths of this length.

The computer data may also be used to tabulate the nondegenerate closed paths of length k inducing the identity permutation. There are no such paths of length $k < 6$, and the paths of length $k = 6, 7, 8$ are unique up to automorphisms of $\mathbb{P}_3$. For $k = 6$, all such paths have the form

$$[0, p, q, 0, p, q, 0]$$

where $0, p, q$ are noncollinear. For $k = 7$, all paths have the form

$$[0, p, r, q, p, r, q, 0]$$

where $0, p, q$ are collinear and r does not lie on their common line. For $k = 8$, all paths have the form

$$[0, p, q, r, p, q, r, p, 0]$$

where $\{0, p, q, r\}$ is an oval. In particular, the number of length-8 paths inducing the identity is the number of ordered ovals beginning with 0, which is $12 \cdot 9 \cdot 4 = 432$. Note that by Proposition 2.2, this is the cardinality of the stabilizer of a point in $\mathrm{Aut}(\mathbb{P}_3) = \mathrm{PGL}_2(\mathbb{F}_3)$.

A striking feature of the depth distribution is that there are only eight permutations at maximal depth. These permutations are

$$\begin{array}{ll} (1\ 3\ 2)(4\ 6\ 5)(7\ 8\ 12), & (1\ 3\ 2)(4\ 5\ 6)(9\ 11\ 10), \\ (1\ 2\ 3)(7\ 8\ 12)(9\ 11\ 10), & (4\ 5\ 6)(7\ 8\ 12)(9\ 10\ 11), \end{array} \tag{6.2}$$

and their inverses. They may be produced respectively by the paths

$$\begin{array}{ll} [\,0, 12, 1, 0, 9, 6, 11, 10, 5, 0\,], & [\,0, 1, 10, 0, 6, 12, 7, 4, 8, 0\,], \\ [\,0, 12, 1, 0, 9, 5, 6, 11, 4, 0\,], & [\,0, 12, 10, 0, 3, 4, 2, 1, 5, 0\,], \end{array}$$

and their reverses. Together with the identity, these eight permutations form an elementary abelian group T. Notice that the orbits of the action of T on $\mathcal{P} \setminus \{0\}$ are the sets $\ell \setminus \{0\}$ for $\ell \in \mathcal{L}(0)$. For any two distinct elements $\sigma, \tau \in T$, there is exactly one line $\ell \in \mathcal{L}(0)$ such that $\sigma(p) = \tau(p)$ for all $p \in \ell$. Thus T is the *tetracode* [Conway:1999, p. 81]. The elements of T are at maximal distance not only from the identity but from each other (because T is a group).

Since $d(\sigma) \leq 9$ for all $\sigma \in M_{13}$, there is a much better algorithm than brute-force search for "solving" the basic game—that is, finding a short path producing a given permutation $\sigma \in M_{13}$. It suffices to consider the case $\sigma \in M_{12}$, since we can always start by moving the hole to 0.

(1) Check if $\sigma \in N$, using the table (6.2). If so, we are done. If not, then $d(\sigma) \leq 8$.

(2) Create a list L_1 of all elements of M_{13} of depth ≤ 4, together with paths realizing them. (An upper bound for the size of this list is $12 \cdot 9^3 = 8748$, the number of paths $[0, p_1, \ldots, p_4]$ with no three consecutive points collinear.)
(3) Create a list $L_2 = \{\sigma^{-1} \circ \tau \mid \tau \in L_1\}$ of all elements of M_{13} at distance ≤ 4 from σ.
(4) Since $d(\sigma) \leq 8$, we must have $L_1 \cap L_2 \neq 0$, i.e., there are permutations τ and τ' such that $\tau = \sigma^{-1}\tau'$. Thus $\sigma = \tau'\tau^{-1}$, and we can construct a path realizing σ by concatenating those for τ' and τ^{-1}.

6.2. **The signed game.** We now study the Cayley graph Γ^+ of the signed game, whose vertices are the $2(13!/7!)$ positions of the signed game and whose edges are given by signed moves. As before, we can define distance, depth, and numbers $[2M_{12}]_k$ and $[2M_{13}]_k$.

Let $\sigma \in M_{13}$, and let σ_1, σ_2 be the two lifts of σ in $2M_{13}$. Then it is easy to see that

$$d(\sigma) \;=\; \min(d(\sigma_1), d(\sigma_2)). \tag{6.3}$$

Proposition 6.2. *The depth distributions for $2M_{12}$ and $2M_{13}$ are given by the following table:*

k	0	1	2	3	4	5	6
$[2M_{12}]_k$	1	0	0	54	540	5184	25821
$[2M_{13}]_k$	1	12	108	918	7344	57852	356949

k	7	8	9	10	11	12
$[2M_{12}]_k$	85230	72351	898	0	0	1
$[2M_{13}]_k$	1192770	843291	11674	108	12	1

The unique element at maximal depth is $-\mathbf{1}$, the permutation that flips every counter in place (see Proposition 3.4). The subgroup $\{\mathbf{1}, -\mathbf{1}\}$ of $2M_{12}$ is central, so every $\sigma \in 2M_{13}$ has a unique "antipode" $-\sigma = -\mathbf{1} \cdot \sigma$, which moves the counters to the same locations as σ but reverses all orientations, and is uniquely maximally distant from σ. Thus Γ^+ may be visualized as a "globe" in which pairs of poles represent antipodal permutations.

The depth distributions for $2M_{12}$ and $2M_{13}$ are the same as those for M_{12} and M_{13} for all depths ≤ 5. Indeed, let k be the smallest number such that $[2M_{13}]_k > [M_{13}]_k$. By (6.3) and the pigeonhole principle, there must be two elements $\sigma_1, \sigma_2 \in 2M_{13}$ at depth $\leq k$ which are lifts of the same $\sigma \in M_{13}$. Then $\sigma_1^{-1}\sigma_2$ is a path of length $\leq 2k$ which induces the permutation $-\mathbf{1}$ in some conjugate of $2M_{12}$, which implies that $d(-\mathbf{1}) \leq 2k$. We must therefore have $k \geq 6$.

We also note that the depth distributions of $2M_{12}$ and $2M_{13}$ are "symmetric near the poles": there are the same numbers of permutations at depths $0, 1, 2$ as at depths $12, 11, 10$ respectively. However, the symmetry breaks down further from the poles: fewer elements of $2M_{13}$ lie at depths $3, 4, 5$ than at depths $9, 8, 7$ respectively. We may partially explain this phenomenon by noting that

$$d(\sigma) + d(-\sigma) \;\geq\; 12, \tag{6.4}$$

for all $\sigma \in 2M_{13}$, for otherwise $-\mathbf{1} = -\sigma \circ \sigma^{-1}$ could be obtained by a path of length strictly less than 12. Moreover, equality holds in (6.4) if and only if some minimal path from σ to $-\sigma$ has $\mathbf{1}$ as an intermediate position, which is not always the case. Thus the mean depth of a permutation is greater than 6.

Once again, these facts are based on the computational observation that $-\mathbf{1}$ is the unique element at depth 12. This observation is also of use in explaining the symmetry of the depth distribution near the poles.

Proposition 6.3. *Let $\sigma \in 2M_{13}$, with $d(\sigma) \in \{1, 2\}$. Then $d(-\sigma) = 12 - d(\sigma)$.*

Proof. Suppose that $d(\sigma) = 1$; then σ is realized by a move sequence $[0, p]$, with $p \neq 0$. Recall from (3.4) that $-\mathbf{1}$ is realized by a length-12 move sequence $[0, \ldots, 5, 6, 3, 0]$. Since $\mathrm{Aut}(\mathbb{P}_3)$ acts doubly transitively on $\mathcal{P}$, we may choose $\alpha \in \mathrm{Aut}(\mathbb{P}_3)$ such that $\alpha(0) = 0$ and $\alpha(3) = p$. Applying α to the move sequence realizing $-\mathbf{1}$, we obtain

$$[0, \ldots, \alpha(5), \alpha(6), p, 0] \tag{6.5}$$

which induces the signed permutation $\alpha \circ -\mathbf{1} \circ \alpha^{-1} = -\mathbf{1}$. Therefore, the path

$$[0, \ldots, \alpha(5), \alpha(6), \alpha(3) = p, 0, p]$$

induces the permutation $-\sigma$. Deleting the last two moves, we obtain an equivalent path of length 11. So $d(\sigma) \leq 11$. The opposite inequality follows from (6.4).

Similarly, if $d(\sigma) = 2$, then σ is realized by a move sequence $[0, p, q]$, with $0, p, q$ noncollinear. By Proposition 2.2 (2), $\mathrm{Aut}(\mathbb{P}_3)$ acts transitively on noncollinear triples of points, so we may choose $\alpha \in \mathrm{Aut}(\mathbb{P}_3)$ such that $\alpha(0) = 0$, $\alpha(3) = p$, and $\alpha(6) = q$. By the same argument as before, $-\sigma$ is realized by the move sequence

$$[0, \ldots, \alpha(5), \alpha(6) = q],$$

which has length 10. □

References

[Archer:1999] Aaron Archer. A modern treatment of the 15 puzzle. *American Mathematical Monthly*, 106:793–799, 1999.

[Cameron:1991] P.J. Cameron and J.H. van Lint. *Designs, Graphs, Codes and Their Links*, volume 22 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[Conway:1985] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *Atlas of Finite Groups*. Oxford University Press, 1985.

[Conway:1987] John H. Conway. Graphs and groups and M_{13}. In *Notes from New York Graph Theory Day XIV*, pages 18–29, 1987.

[Conway:1997] J.H. Conway. M_{13}. In *Surveys in combinatorics, 1997 (London)*, volume 241 of *London Mathematical Society Lecture Note Series*, pages 1–11. Cambridge University Press, Cambridge, 1997.

[Conway:1999] John H. Conway and Neil J.A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 3rd edition, 1999.

[Martin:1996] Jeremy L. Martin. The Mathieu group M_{12} and Conway's M_{13}-game. Undergraduate thesis, Harvard University, 1996.

Department of Mathematics, Princeton University, Princeton, NJ 08544

Department of Mathematics, Harvard University, Cambridge, MA 02138
E-mail address: elkies@math.harvard.edu

Department of Mathematics, University of Kansas, Lawrence, KS 66045
E-mail address: jmartin@math.ku.edu