

A Finite Simple Puzzle of Order 44,352,000

Erica Chesley, Zack Starer-Stor, Emma Zhou

Abstract

The Rubik's cube and Loyd's fifteen-puzzle are familiar examples of puzzles which have an underlying group structure. We designed a new puzzle based on the Higman-Sims group (HS), one of the illustrious twenty-six sporadic simple groups. Our puzzle gave us a concrete representation of HS, which we used to gain deeper insight into the structure of the group; at the same time, we were able to use our knowledge of HS to solve our new puzzle. In this paper we debut the latest puzzle craze, discuss our results concerning some of its subpuzzles, and demonstrate a solution.

1 Background

Throughout human history, solving puzzles and playing games have gone hand-in-hand with the development of mathematics. In 1735, on a visit to the town of Königsberg, Russia, Euler solved its citizens' long-standing bridge puzzle, and began the discovery of graph theory. In 1654, when the Chevalier de Mere asked mathematician Blaise Pascal about the strategy associated with a particular dice game, the latter's subsequent correspondences with Pierre de Fermat led to the development of probability theory. Several ancient texts testify to explorations in counting and combining which were eventually formalized as the mathematical subdiscipline of combinatorics. The oldest known example of one of these puzzles appears in the Bhagabati Sutra from ancient India and asks how many combinations of any size can be made from six different tastes.

Group theory is no exception to this partnership. You may well be familiar with Sam Lloyd's 15-puzzle, in which tiles numbered one through fifteen are arranged in a four by four grid, with a blank space in the bottom right corner, in increasing consecutive order except that the fourteen tile and the fifteen tile are swapped. The goal is to slide the tiles (by moving tiles adjacent to the blank space into the blank space and thus opening a new blank) in such a way that you are left with all the tiles arranged in full ascending numerical order, and the blank is back in the bottom right corner.

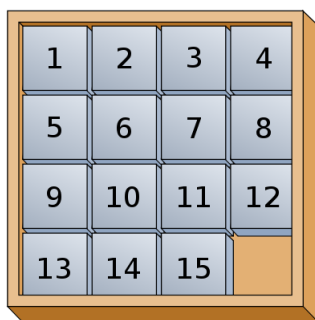


Figure 1: The Fifteen Puzzle

Now, it turns out that the 15-puzzle is an instantiation of the alternating group A_{15} because every move consists of exchanging the blank space with an adjacent tile enough times to return the blank to its corner. If we color the tiles of the fifteen-puzzle in the style of a checkerboard (alternating colors), we can see that any swap takes the blank tile to the other color than it is currently on, which forces it to take an even number of exchanges in order to return to the same color, or same space, that it started on (you will recall that the alternating group A_n is the subgroup of all permutations of n elements known as the symmetric group S_n

which can be rewritten as the product of an even number of two-cycles). I will leave it to you to take the final step from this observation to a conclusion about solving the puzzle itself.



Figure 2: The Fifteen Puzzle with Checkerboard Coloring

A puzzle that you’re even more likely to have heard of, played with or even solved is that plastic cube with the solid colored stickers all over it – the Rubik’s Cube. The Rubik’s Group, or set of achievable states of the Rubik’s Cube, can be similarly described in terms of symmetric and alternating groups.

You have noticed, perhaps, that all of the above group/puzzle correlations went in the same direction, that is, that in each case, chronologically, the puzzle came first and then someone noticed the relationship that the puzzle bore to a group, and used their understanding of that group to solve or develop or modify the puzzle. Why not try going in the opposite direction? No reason.

In July 2008, Scientific American published an article [6] by Igor Kriz and Paul Siegel, a professor and student respectively, at the University of Michigan, who had done just that. They had noticed that because most derivative, or “copycat,” puzzles from the Rubik’s Cube became relatively easy to solve once an individual had solved the Rubik’s Cube itself, because they were built from the same sorts of symmetric and alternating groups. (Which does speak rather loudly to the strength of the parallel between the puzzles and their associated groups – if solvers could intuit an understanding of the group by default of understanding the one puzzle that carried over to an understand in the solver of other puzzles.) In commenting on the extensive applications of group theory in such fields as crystallography, elementary particle physics, string theory and even in telecommunications, they claim that puzzling out a solution to Rubik’s Cube has turned out to be a terrific way for people to get a feel for the ways that the elements of certain kinds of abstract groups combine. The idea for them, then, was to offer a means of connecting with more abstract groups. Happily, the experiences of our colleagues show that anyone who can learn to solve Rubik’s Cube can gain an equally substantial understanding of these sporadic groups by doing our puzzles.

The groups they chose to work with come from a set of groups known as the sporadic simple groups. For those who might not know, simple groups are those with no proper, normal subgroups (i.e. no subgroups different from the group itself having the property that any element of the group composed with any element of the subgroup composed with the inverse of the first element is some element of the subgroup). By the current classification of simple groups, there are eighteen families of finite simple groups, and twenty-six finite simple groups that don’t fit into these families – these are the sporadic simple groups. Kriz and Siegel chose two sporadic simple groups discovered by Emile Mathieu, the groups M_{12} and M_{24} , and one discovered by John Conway, Co_0 , to make their puzzles from. Knowledge of key facts about these groups, such as the property of M_{12} and M_{24} of being five-transitive (that is, that any five points can be taken to any five position by some permutation in the group), significantly aids in the solution of the puzzles, in the case of the Mathieu groups by telling the solver to search for a sequence of moves that shifts five of the numbers to any five positions in the puzzle while fixing the rest of the puzzle. And familiarity with the puzzles offers a deeper level of comfort with these abstract groups, in much the same way that familiarity with sharing twelve cookies among three friends and oneself and familiarity with the algorithm for dividing twelve by three plus one supplement one another.

Two years earlier than Kriz and Siegel, Conway, Elkies and Martin published the article “The Mathieu Group M_{12} and its Pseudogroup Extension M_{13} ” [2] in which they describe a different puzzle, analogous to the fifteen-puzzle, whose achievable states also model the elements of the Mathieu M_{12} group. In this puzzle, the positions are those of the projective plane of order three (see Figure 3, below), in which every one of thirteen “lines” contains four distinct points, and every one of thirteen points is contained in exactly four lines.

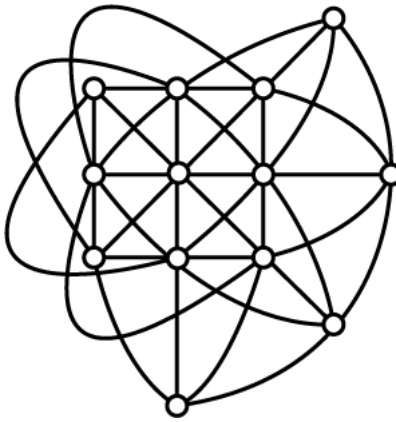


Figure 3: The Projective Plane of Order Three

The positions are numbered 0 through 13, and every position other than “0” gets a counter of the same number placed on it in the solved state. A move is defined by the current position of the blank and by some counter that is currently collinear with it. The move is executed by moving that counter to the blank space (effectively, “putting” the blank in that counter’s position), as well as exchanging the positions of the other two counters on the line containing the two elements defining the move (which, by definition of the projective plane, is unique).

The three authors define also a “signed” alternative version of this game, which they prove is isomorphic to “the non-trivial double cover $2 M_{12}$ ” and that the group represented by this game mod Z is isomorphic to M_{12} . Next, they construct yet another game (this time, the “Dualized game”) from that original puzzle, show that it is isomorphic to the original, and therefore to M_{12} , and define an outer automorphism of the new game, thereby offering a representation of an outer automorphism of M_{12} and a more concrete understanding of the automorphism group of M_{12} . Here, rather than using knowledge of a group to solve a puzzle, Conway, Elkies and Martin use a puzzle to increase knowledge of a group.

2 An Early Puzzle

Along with the preexisting groups that we studied, we looked at the group structure of several puzzles that we invented. The most significant of these was a family of shifting square puzzles. The 5×5 case is shown below:

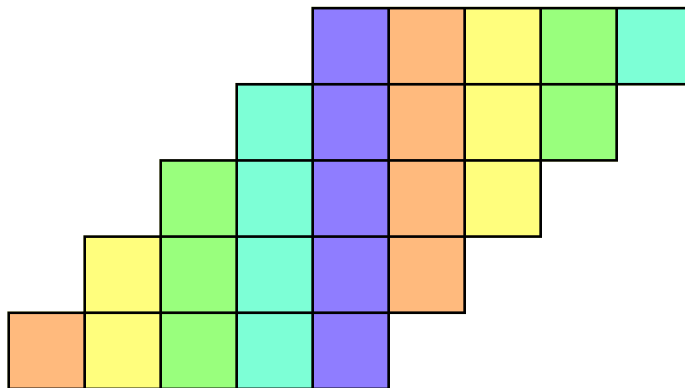


Figure 4: The 5×5 Shifting Square Puzzle

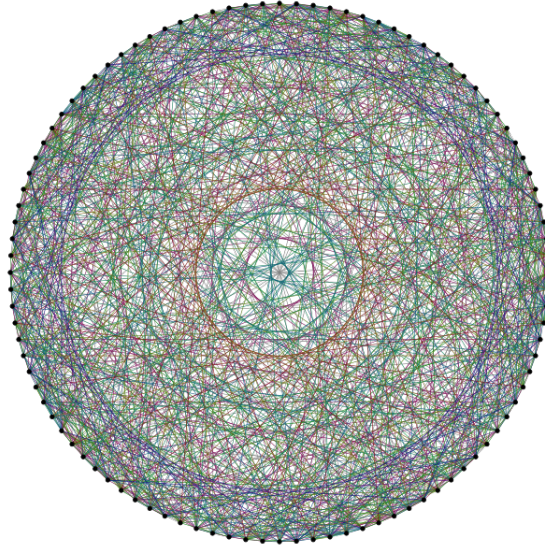


Figure 5: The Higman-Sims Graph

These puzzles are characterized by two moves: a horizontal shift and a vertical shift. Both moves wrap, that is, a shift right will take all of the pieces on the far right side of the puzzle to the far left side. The family consists of any boards made up of squares that use these two moves.

This is an area for future study, as we primarily looked at the above case, and our findings, while convincing, are not rigorously proven.

The 5×5 board has order 62,208,000,000, or $\frac{1}{2} \times 5 \times (5!)^5$. This is important, because it is from this number that we derive our intuition.

The group is imprimitive: the colors in the above figure denote blocks, as the vertical shift permutes elements of each block amongst themselves, and the horizontal shift cycles between block positions. If we could find any ordering within each of these blocks, each would have $5!$ states possible, so our total number of states for these five blocks would be $(5!)^5$. This is multiplied by 5 because there are 5 positions that the blocks can be placed in each of the above colors. The $\frac{1}{2}$ then should signify that the specific group generated by this puzzles only contains even permutations.

3 The Higman-Sims Graph and Group

Having explored the relationship between groups and games a bit in the game to group direction, we shifted our focus and selected a group that we found interesting but wanted to gain further insight into. The group we chose is the Higman-Sims group, a sporadic simple group of order 44,352,000 which acts on 100 points. The Higman-Sims group comes out of the automorphism group of the Higman-Sims graph, which acts on 100 vertices. The Higman-Sims graph is regular of degree 22, and has no triangles. That is, two adjacent vertices have no neighbors in common. Additionally, the graph has the property that two non-adjacent vertices have 6 neighbors in common.

The automorphism group of this graph has order 88,704,000, and HS is isomorphic to a subgroup of this automorphism group with index 2. The result is a sporadic group of order 44,352,000. This group can be represented as the automorphism group of a Steiner system $S(3, 6, 22)$, which has blocks of size 6 acting on a set of 22 points so that any 3 points is contained in exactly one block. Since any three points determine a block, the largest feasible number of blocks would be $22 \times 21 \times 20$. However, order does not matter, so we can divide by $3! = 6$, and since there are six points that we could have used to fix, we can divide by $\binom{6}{3} = 20$, as any three of the six points would do. This number works out to 77, and indeed the group has 22 points, 77 blocks, and one point, labeled * in Higman and Sims's original 1967 paper [5]. These are our 100 vertices. The Higman-Sims Graph is constructed by defining an edge between * and every vertex corresponding to a

point, as well as between every vertex corresponding to a point and every vertex corresponding to a block in which that point is contained. The HS group has subdegrees of 1, 22, and 77, which corresponds to our three types of vertices: *, points, and blocks.

This group is strongly related to M_{22} . In fact, if we fix any one of the vertices on our graph, the resulting group is M_{22} . This is not entirely surprising, as the order of M_{22} is 443,520, which is one hundredth of the size of Higman-Sims. Since we fix one of our 100 points to get M_{22} , this relationship of the orders makes sense. We will discuss this point-stabilizer in more depth in describing our method for solving the puzzle later in this paper.

Higman-Sims has a number of different constructions. N.L. Biggs and A.T. White [1] published a projective plane approach, and Paul R. Hafner [4] and R. Mathon & A.P. Street [7] published separate elementary constructions of the group. However, in this paper we use the original permutations put forth by Higman and Sims in their 1967 paper.

$$\begin{aligned}
 a = & (2, 8, 13, 17, 20, 22, 7)(3, 9, 14, 18, 21, 6, 12)(4, 10, 15, 19, 5, 11, 16)(24, 77, 99, 72, 64, 82, 40) \\
 & (25, 92, 49, 88, 28, 65, 90)(26, 41, 70, 98, 91, 38, 75)(27, 55, 43, 78, 86, 87, 45) \\
 & (29, 69, 59, 79, 76, 35, 67)(30, 39, 42, 81, 36, 57, 89)(31, 93, 62, 44, 73, 71, 50) \\
 & (32, 53, 85, 60, 51, 96, 83)(33, 37, 58, 46, 84, 100, 56)(34, 94, 80, 61, 97, 48, 68) \\
 & (47, 95, 66, 74, 52, 54, 63)
 \end{aligned}$$

$$\begin{aligned}
 b = & (1, 35)(3, 81)(4, 95)(6, 60)(7, 59)(8, 46)(9, 70)(10, 91)(11, 18)(12, 66)(13, 55)(14, 85)(15, 90) \\
 & (17, 53)(19, 45)(20, 68)(21, 69)(23, 84)(24, 34)(25, 31)(26, 32)(37, 39)(38, 42)(40, 41)(43, 44) \\
 & (49, 64)(50, 63)(51, 52)(54, 95)(56, 96)(57, 100)(58, 97)(61, 62)(65, 82)(67, 83)(71, 98)(72, 99) \\
 & (74, 77)(76, 78)(87, 89)
 \end{aligned}$$

4 The Higman-Sims Puzzle

In order to gain a more intuitive and less abstract understanding of the Higman-Sims group, we used the permutation representation given by Higman and Sims to create a puzzle whose achievable states correspond to the group elements of the Higman-Sims group. This gave us a concrete version of the group with which to interact and learn from.

How the puzzle works

Cycle: Cycle takes every 7-cycle and rotates it by 1. Positions L and R are left unchanged.

Swap: note that every position on every cycle has a spoke on it that is a different color. Swap takes whatever is in that position and switches it into the cycle of corresponding color, replacing whatever was in the opposite position in that cycle.

Reset: Resets the game.

Randomize: Takes you to a pseudorandom configuration by doing some sequence of Cycles and Swaps.

Custom buttons: To define a custom button, click on it once, then do some sequence of moves that can include Cycle, Swap, and other custom buttons. When you are done, click the custom button again. It is now set, and every time you click it, it will do your sequence of moves. To empty a custom button, click on the white X in the top right corner.

5 Simplicity of the Higman-Sims Group

Proof that the Higman-Sims group is simple (expanded from the proof outlined in Wilson [8]). We take as given that the point-stabilizer of HS is M_{22} , and that M_{22} is a simple group.

Lemma 5.1. *HS acts primitively on one hundred points.*

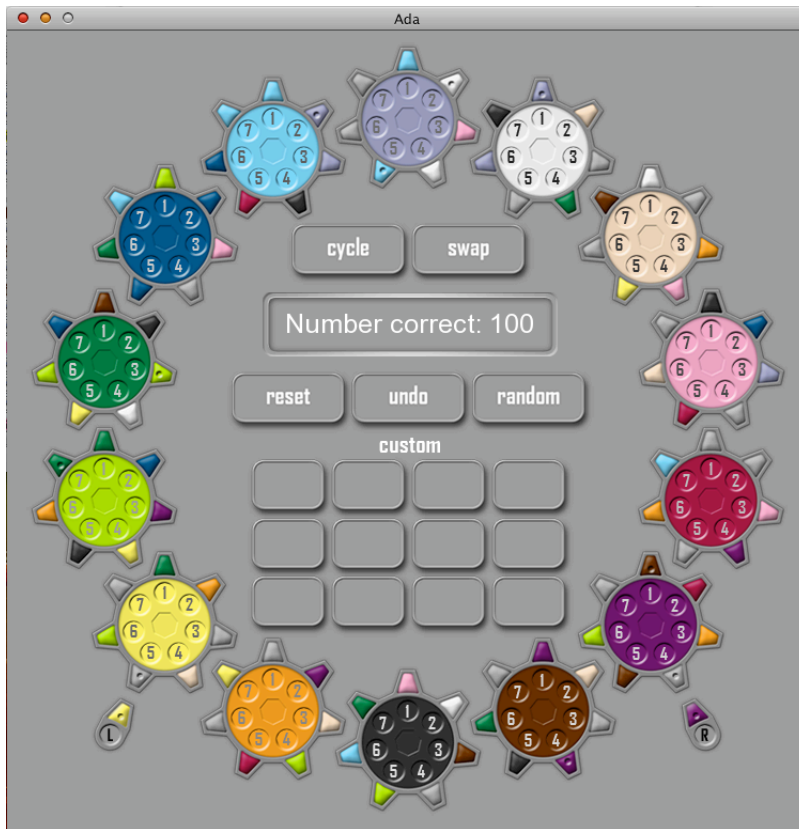


Figure 6: The Higman-Sims Puzzle

Proof. We know from the construction of the Higman-Sims group from the Higman-Sims graph that HS acts on one hundred point. Suppose that HS is imprimitive on those hundred points. Then there exists some partition of the hundred points into equal-sized blocks (containing more than one element each, and fewer than the entire group) such that for all points α and β and all permutations $\pi \in HS$, if α and β are elements of the same block, then α^π and β^π are elements of the same block as well. We consider two possible cases.

Case i. Our partition has no blocks that contain more than one element from the same cycle.

Then the cycle permutation moves every point, excepting L and R, to a different block, while fixing L and R in their initial blocks, so L and R cannot share a block with any numbered positions, so L and R must form a block together and our partition must be into blocks of order two.

Then any permutation that fixes L must also fix R, but the permutation sc^5sc^2s fixes L and moves R to the dark green six position. So we have a contradiction.

Case ii. There exists a block in the partition that contains two spaces, call them α and β , from the same cycle.

Then there must exist some permutation c^i , consisting of i cycles, where $1 \leq i \leq 6$ that takes α to β . Because it takes α to a point in the same block, c^i must preserve the block. But seven is prime, so c^i generates the entire cycle, and the entire cycle, therefore, is in the same block under consideration. Furthermore, if any point from another cycle is in this block, that entire cycle must also be in the block, because the cycle move preserves the block.

So our partition of the points must be into blocks of size $7k$, $7k + 1$ (if L or R is in this block) or $7k + 2$ (if L and R are in this block). The only number of one of these form that also divides 100 is $50 = 7 \times 7 + 1$. Our partition is into two blocks of size 50 each, where each block contains seven cycles and the L or the R. So L and R are in different blocks, so the spaces that swap takes them to (yellow five and purple four) must also be in different blocks. But each cycle must be in only one block, so the entire yellow and purple cycles must be in different blocks. Any positions that points from those two cycles (such as yellow two and purple

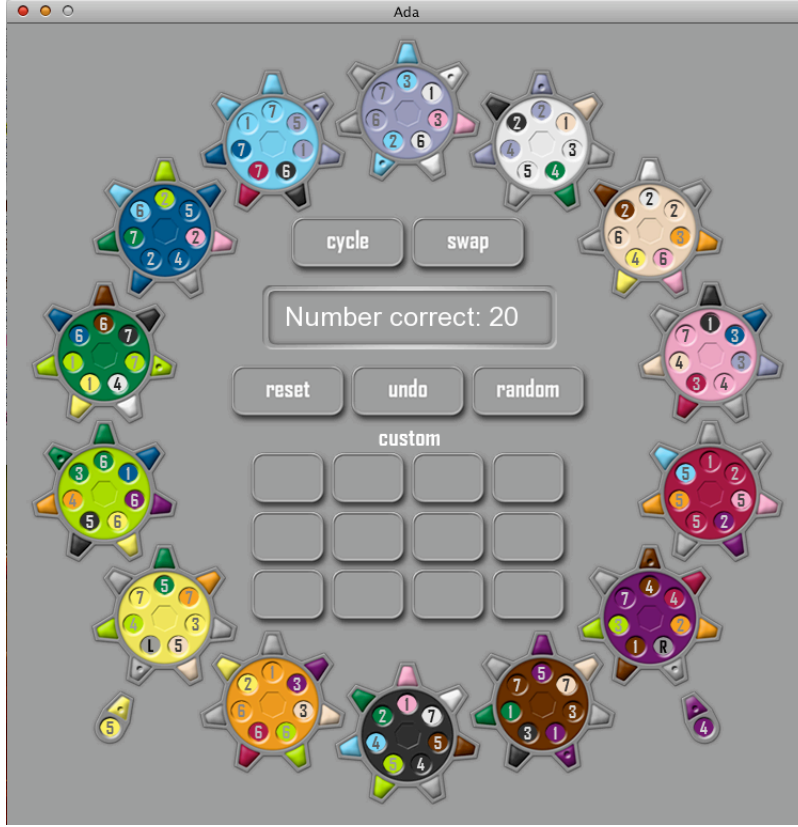


Figure 7: The Higman-Sims Puzzle After One Swap

three) swap into (in this case, orange seven and orange two) must also be in different blocks. So orange two and orange seven must be in different blocks, but the entire orange cycle must be in only one block. Contradiction.

HS cannot be imprimitive. HS must therefore be primitive, and more specifically, must act primitively on the one hundred points. \square

Lemma 5.2. *Any non-trivial proper normal subgroup N of HS is transitive on the hundred points.*

Proof. We proceed by contradiction. Suppose that N is not transitive on the hundred points. Then the orbits of the hundred points under N form disjoint subsets of the points. Take α, β of the same orbit in N . Then there exists some $n \in N$ such that $n(\alpha) = \beta$. Because N is normal in HS , then for every $h \in HS$, there must exist some $m \in N$ such that $mh = hn$. Then $mh(\alpha) = hn(\alpha) = h(\beta)$. So for every $h \in HS$, $h(\alpha)$ and $h(\beta)$ must be contained in the same orbit under N . The orbits of N therefore form a system of imprimitivity in HS . But HS is primitive, so we have a contradiction, and N must be transitive on the hundred points. \square

Lemma 5.3. *Any non-trivial proper normal subgroup N of HS intersects HS trivially, and has order 100.*

Proof. For any $x \in M_{22}$, we have $x(N \cap M_{22})x^{-1} = xNx^{-1} \cap xM_{22}x^{-1}$. But N is normal in HS and every element of M_{22} is an element of HS , so $xNx^{-1} = N$. And x and x^{-1} are elements of M_{22} so $xM_{22}x^{-1} = M_{22}$. Therefore $x(N \cap M_{22})x^{-1} \subseteq N \cap M_{22}$, and $N \cap M_{22}$ is normal in M_{22} . But M_{22} is simple, so has no proper normal subgroups. $N \cap M_{22}$ must therefore be either all of M_{22} or $\{e\}$, that is, N intersects M_{22} trivially.

Suppose the intersection of N and M_{22} is all of M_{22} , that is, $M_{22} \subseteq N \subseteq HS$. Then N/M_{22} is the set of cosets of M_{22} in N . Because M_{22} is the point-stabilizer in N , every element of a given coset always sends some point, say L , to the same position. But because N is transitive (by Lemma 5.2), for every position in our hundred points, there exists some permutation in N that will send L to that position, so the order of

N/M_{22} must be at least 100. So $|N| \leq 100 \cdot |M_{22}| = |HS|$ and N must be HS . But N was defined as a proper subgroup of HS , so we have a contradiction. The intersection of N with M_{22} must be $\{e\}$.

Because N is transitive on the hundred points, we know that $|N| \geq 100$. Now, $|NM_{22}| = |N||M_{22}|/|N \cap M_{22}| = |N||M_{22}|/1 = |N||M_{22}|$ and $NM_{22} \subseteq HS$, so $|N||M_{22}| \leq |HS|$ and $|HS| = 44,352,000$ and $|M_{22}| = 443,520$. So $|N| \leq 100$. N must have order 100. \square

Lemma 5.4. *Any non-trivial proper normal subgroup N of HS has a subgroup H of order 25, which is normal in HS .*

Proof. By Lemma 5.3, N has order $100 = 5^2 \times 4$, where 5 is prime and 4 is not divisible by 5, so by the Sylow theorems, N has at least one subgroup of order $5^2 = 25$, call it H .

Now, $xNx^{-1} = N$ implies that there exists an automorphism φ of N defined by $\varphi(n) = xnx^{-1}$ for all $n \in N$. Because H is a characteristic subgroup of N , it is preserved by any automorphism of N , so $\varphi(H) = H$, and $xHx^{-1} = H$. H is normal in HS . \square

Theorem 5.5. *The Higman-Sims group HS is a simple group.*

Proof. By Lemma 5.3 above, any normal subgroup N of HS has order 100. By Lemma 5.4, this subgroup N must have its own subgroup H of order 25, which is also normal in HS . Again by Lemma 5.3, H must therefore have order 100. This is a contradiction. HS therefore cannot have any proper normal subgroups. By definition, the Higman-Sims group must be simple. \square

6 Subpuzzles of the Higman-Sims Puzzle

A single seven-cycle (1 swap): The order of this group is 40,320. It is possible to switch any two elements using the following method: using some combination of swaps and cycles, move the first element into the 8 spot. Then, using only cycles (which leaves the first element fixed), move the second element into the 1 spot. Then swap the first and second elements. Finally, using only cycles again, move whatever ended up in the first element's spot into the 1 spot, then swap that element and the first element. Since it is possible to swap any two elements in this way, and any permutation of n elements can be written as a collection of two-cycles, every state is reachable in this subpuzzle. Thus, the group must be S_8 , which has order $8!$.

A single seven-cycle (7 swaps): The order of this group is 98. Note that when cycling or swapping, the "inner" and "outer" rings stay completely disjoint. That is, they are in different blocks. However, both are able to (independently) cycle through seven positions. Furthermore, they are either swapped, or not swapped. That makes $7^2 \times 2$ achievable states. The group underlying this puzzle is $Z_7 \wr Z_2$.

A single seven-cycle (6 swaps): The order of this group is 3,113,510,400. Every adjacent three cycle is possible (that is, it's possible to cycle only 1, 2, and 3), and from this, we can show that every three cycle in general is possible. Since every three cycle is made of two two-cycles, we can achieve only the even permutations of 13 elements, which means the group must be A_{13} .

Two seven-cycles (1 swap): The order of this group is 896. Let a_1 =swap, and c =cycle. Let $a_n = ca_{n-1}c^{-1}$. Note that the groups generated by $\langle a_1 \dots a_n \rangle$ are the power sets of (a_1, a_2, \dots, a_n) , so $|\langle a_1 \dots a_n \rangle|$ must be 2^7 . Additionally, there are seven positions to cycle through, thus, 7×2^7 . This group is the alternating subgroup of $S_2 \wr Z_7$.

Three seven-cycles (2 swaps): The order of this group is 979,776. To show this, first pretend that in addition to swap and cycle, we have a third move, which we will call switch. The third move simply takes everything in the first cycle, and switches it with its corresponding thing in the third cycle. The new group that we've generated has order $3!^7 \times 7$. Since our original group was the alternating group of this new group, it must have order $(3!^7 \times 7)/2$.

7 Solving the Puzzle

Knowledge of the structure of HS relative to the other Sporadic groups is crucial in the solution of our puzzle. In fact, we derive a solution through a series of point-stabilizations, finding generators for the groups that arise and essentially solving the resulting smaller puzzle in a similar manner.

We use the following groups in the solution:

$$|HS| = 44,352,000 = 100 \times 22 \times 21 \times 20 \times 48$$

$$|M_{22}| = 443,520 = 22 \times 21 \times 20 \times 48$$

$$|M_{21}| = 21,160 = 21 \times 20 \times 48$$

$$|M_{20}| = 960 = 20 \times 48$$

M_{22} is the point stabilizer of HS , so we look to find moves that fix one point of the Higman Sims puzzle, and from these generate M_{22} .

Let X represent a sequence of cycles and swaps in our game:

$$X = CSC^5SC^6SC^4SC^2$$

The Atlas of Finite Group representations gives us an algorithm for generating M_{22} : X has order 8, so we take its square, $Y = X^2$. We also take the square of Y , $Z = Y^2$. We conjugate Y and Z to find A_0 and B_0 respectively, so that A_0B_0 has order 11, and $A_0B_0A_0B_0B_0$ has order 11[9].

We define

$$U = C^2S$$

$$V = C^4SC^3SCSCSC^2SCSCSC^4$$

Then if we let $A_0 = UZU^{11}$, and $B_0 = V^3YV^8$, A_0 and B_0 generate M_{22} .

These generators fix the Tan 1 spot in our puzzle. However, because of the unique nature of the * spot in the construction of the game, there are more interesting results to be found by fixing this place instead. In our puzzle this is represented by the L spot. So, we can fix L instead of Tan 1 by conjugating our moves again. By moving L to Tan 1, performing our operations, and moving Tan 1 back to L , we still generate M_{22} , and we fulfill the objective of fixing L .

$$W = SC^6SC^3$$

$$A = WA_0W^6$$

$$B = WB_0W^6$$

A and B generate M_{22} , fixing L . To solve, we move L into place using our standard operations, and then use only moves that fix L .

This gives us M_{22} represented over 99 points. Three cycles, Orange, White, and Dark Green, as well as the R spot, are now self contained. This is the classic 22 point representation of M_{22} . The other cycles permute amongst themselves in a 77 point representation. Thus, our puzzle gives a one-to-one correspondence between states in these two representations, as the point stabilizer of HS is just M_{22} - HS does not point stabilize into two independent copies of M_{22} .

Because both sets of points represent the same group, it is sufficient to solve the 22 point representation of M_{22} , so in the solution of the puzzle we can ignore the 77 point representation.

The point stabilizer of M_{22} is M_{21} , or $PSL(3,4)$. Generators of M_{21} are P , Q , such that P has order 2, Q has order 4, PQ has order 7, and PQQ has order 5[9].

$$T = (AB)(ABABB)^6A$$

$$S = (AB)(ABABB)(AB)(ABABB)(AB)$$

$$P = BAB^3$$

$$Q = TST^3$$

P and Q generate M_{21} . These operations produce the point stabilizer of M_{22} by fixing R . So, if we use combinations of A and B to move R into place, we can then restrict possible moves to combinations of P and Q , leaving L and R fixed. Usefully, the cycle operation is still relevant, as it fixes L and R by definition. This makes it considerably easier in later steps to move $O6$ into place for stabilization.

So, we have a natural, 21 point representation of M_{21} on the Orange, White, and Dark Green cycles. However, the 77 point representation of M_{22} breaks down, separating into another natural representation of M_{21} , on the Black, Light Green, and Magenta cycles, and a 56 point representation of M_{21} on the remaining eight cycles. This gives us another set of one-to-one correspondences between states in different representations of a group, this time between states in M_{21} .

The point stabilizer of M_{21} is M_{20} , equivalent to $16:A_5$. M_{20} is generated by I and J , where I has order 4, J has order 3, and IJ has order 5[9]. We define:

$$I = QPC^2$$

$$J = PQPC^3$$

I and J stabilize $O6$, resulting in a 20 point representation of M_{20} over the remainder of the Orange, White, and Dark Green cycles. While we did not examine this closely, it appears that the other 21 point representation of M_{21} breaks down into a 5 point representation of A_5 (Black 1, Black 3, Black 4, Light Green 3, and Magenta 5) and a 16 point representation of M_{20} . Our solution solves a copy of A_5 embedded in the block structure of the 20 point representation of M_{20} , but it seems likely that we could have solved more simply by looking at this representation of A_5 . We did not examine the behavior of the remaining 56 points, and this is an area that could be explored in the future, as it has the potential to provide a large number of correspondences between different representations of M_{20} .

M_{20} is comprised of five blocks of four objects. These blocks are permuted according to A_5 - the four objects within the blocks make M_{20} the sixteenfold cover of A_5 . To solve, we first manipulate the blocks into their correct places, and then focus on the points within them.

The blocks are:

$$\alpha = (W4, DG2, DG3, DG5)$$

$$\beta = (W1, W5, W6, DG1)$$

$$\gamma = (O2, O7, W3, DG7)$$

$$\delta = (O3, O4, W7, DG4)$$

$$\epsilon = (O1, O5, W2, DG6)$$

We start by fixing γ . It is then helpful to define additional moves that permute these blocks.

$$M = IJI$$

$$N = (IJ)^2M(IJ)^3$$

Using M and N , we find that the following moves permute:

$$M : (\alpha \beta \epsilon)$$

$$N : (\alpha \delta \epsilon)$$

$$NM^2 : (\alpha \beta \delta)$$

$$M^2N : (\beta \delta \epsilon)$$

$$MN : (\alpha \beta)(\delta \epsilon)$$

$$NM : (\alpha \delta)(\beta \epsilon)$$

$$M^2NM^2 : (\alpha \epsilon)(\beta \delta)$$

We can use these to fix any configuration of the blocks so long as γ is fixed, as only even permutations are possible in A_5 .

We did not determine the structure of the group where all blocks are fixed or the structure of the group within these individual blocks. This is an area where future study would come in use, as although we are able to solve using these techniques, we do not know with certainty that the subsequent moves actually generate the groups we use them to solve.

Since I^2 fixes all blocks, we conjugate I^2 to find other moves that fix all blocks. We focus first on solving γ , so only the effect of these moves on the objects within γ are listed. Each move has consequences on the objects within the other blocks as well, but we focus first on solving within γ .

$$I^2 : (O2 DG7)(O7 W3)$$

$$(IJ)^2I^2(IJ)^3 : (O2 W3)(O7 DG7)$$

We then find moves that fix the objects within γ , which allows us to find a solution. This is essentially equivalent to a point stabilization we have stabilized the γ block entirely, both in its block position and in the pieces making up the block.

The effects of the following moves are grouped by the blocks they modify:

$$(I^2)(JI^2J^2) : (W4 DG2)(DG3 DG5) (W1 W5)(W6 DG1) (O3 W7)(O4 DG4) (O1 W2)(O5 DG6)$$

$$(JI)^3I^2(JI)^2 : (W4 DG3)(DG2 DG5) (W1 W6)(W5 DG1) (O3 DG4)(O4 W7) (O1 DG6)(O5 W2)$$

These provide the final moves necessary to solve the puzzle.

8 Conclusions/Further Studies

If we had more time, we would have liked to study more subpuzzles of the HS puzzle, to figure out what groups underlie them, and whether there is a general formula to be derived there. We could have turned cycles "on" and "off" in the game, for example, or simply taken cycles out of the game altogether. We also could have added cycles, or changed the permutation underlying the swap button. We might have removed Left and Right altogether, or added more special positions.

We might also have turned our attention to figuring out how to more easily figure out the group underlying a game. Given an arbitrary game, how do you represent it symbolically? Does every game draw from a finite set of moves? And once you've represented it, how do you then figure out the group underlying it?

There's also much work to be done in some of the other sporadic groups, to try and create games out of them. We believe that our game gave us a much deeper and more intuitive understanding of the structure of the underlying group, and a game created from a different group would do the same for that group.

References

- [1] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, Cambridge University Press, 1979.
- [2] John H. Conway, Noam D. Elkies, and Jeremy L. Martin, The Mathieu Group M_{12} and Its Pseudogroup Extension M_{13} , *Exp. Math.* **15**(2006), No. 2, 223–236.
- [3] Joseph A. Gallian, *Contemporary Abstract Algebra, 7th edition*, Brooks/Cole, Cengage Learning, 2010.
- [4] Paul R. Hafner, On The Graphs of Hoffman-Singleton and Higman-Sims, *Electron. J. Combin.*, **11**(2004), 1–33.
- [5] D. G. Higman and C. C. Sims, A Simple Group of Order 44,352,000, *Math. Z.* **105**(1968), 110–113.
- [6] Igor Kriz and Paul Siegel, Simple Groups at Play, *Sci. Am.* July 2008, 84–89.
- [7] R. Mathon and A. P. Street, Partitions of sets of two-fold triple systems, and their relation to some strongly regular graphs, *Graphs Combin.* **11**(4); 347–366, 1998,
- [8] Robert A. Wilson, *The Finite Simple Groups*, Springer, 2009.
- [9] The Atlas of Finite Group Representations, <http://brauer.maths.qmul.ac.uk/Atlas/v3/>

Images

Figure 1: commons.wikimedia.org/wiki/File:15-puzzle.svg

Figure 2: www.puzzleworld.org/puzzleworld/puz/fifteen_puzzle.htm

Figure 3: home.wlu.edu/~mcraea/Finite_Geometry/NoneuclideanGeometry/Prob14ProjPlane/problem14.html

Figure 5: commons.wikimedia.org/wiki/File:Higman_Sims_Graph.svg