Review: "Build a Sporadic Group in Your Basement"

Parker Hyde

Georgia State University, Mathematics and Statistics Department, Atlanta, 30302, U.S.A

Email: phyde1@student.gsu.edu

ABSTRACT

Example Abstract. Abstract must not include subheadings or citations. Example Abstract. Abstract must not include subheadings or citations. Example Abstract. Abstract must not include subheadings or citations. Example Abstract. Abstract must not include subheadings or citations. Example Abstract. Abstract must not include subheadings or citations. Example Abstract. Abstract must not include subheadings or citations. Example Abstract. Abstract must not include subheadings or citations.

Introduction

Any undergraduate student who has completed a course in abstract algebra will likely be familiar with the notion of a normal subgroup. A typical introductory textbook will introduce this concept early and emphasize its importance to fundamental ideas such as homomorphisms, cosets, and Lagrange's Theorem. The relationship between normal groups and factor groups is often especially emphasized. Readers of I.N. Hernstein's Topics in Algebra, for example, will see a variety of examples in which a normal subgroup N of a groups G, yields a factor group G/N comprised of cosets from the original group G.

The group of residue classes modulo 5, denoted by Z5, provides a particularly accessible example of this. This group can be obtained as a factor group, Z/5Z, from the group of integers Z with its associated normal subgroup 5Z. Reflecting on this example, an observant student might recognize that the group Z seems to permit a decomposition into a product of 'simpler' groups 5Z and Z5 in the way that composite numbers can be decomposed into a product of smaller numbers. The student might further notice that Lagrange's Theorem forbids Z5 from having such a decomposition of its own due to its prime order. This might suggest that Z5, a cyclic group of order 5, is analogous to a prime number whose only factors are trivial. Thus the student may reasonably conclude that Z5 is some kind of special simple group in the sense that it is a finite group whose only proper normal subgroup is the trivial group. Indeed, such groups are called "finite simple groups" and they are of incredible importance in the modern mathematics landscape.

Tremendous effort and volumes of mathematical literature have been exhausted in trying to understand the so-called finite simple groups. A very large subset of this work, composed of over 10,000 pages written by more than 100 mathematicians, simply establishes a comprehensive classification of the finite simple groups. Many mathematicians agree that this work is valid. The results show that almost every simple group falls into 1 or 18 infinite families[]. The first infinite family contains the group Z5 mentioned in out toy example above. In fact, it is comprised of all the cyclic groups of prime order. The second infinite family contains all alternating groups An, where n>=5. The remaining 16 families are the groups of Lie type which are considerably more complex. Fascinatingly though, there exists 26 outlier simple groups known as the sporadic groups which fail to fit into any of these infinite families.

The first 5 of these 26 exceptions to the rule were discovered by mathematician Emile Mathieu in 1873 and are appropriately named The Mathieu groups. Individually, the Mathieu groups are denoted $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ where the subscripts signify that the Mathieu group M_n is a permutation group on n elements. The group M_{24} was originally instantiated by Mathieu as the the particular subgroup of S_{24} generated by the 3 arbitrary permutations:

$$
\begin{aligned}
a &= (1,2,3,...,23)\\
b &= (3,17,10,7,9)(5,4,13,14,19)(11,12,23,8,18)(21,16,15,20,22)\\
c &= (1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)...(8,14)(9,21)(11,17)(13,22)(19,15)
\end{aligned}
$$

This representation is generally opaque and leaves much to be desired for a mathematician seeking a more natural construction. R.T Curtis, who presnted M_{24} as group actions on an icosatetrahedron, stated that the construction was "clever" but "hardly natural."

Modern constructions of M_{24} are often defined as the automorphism group on one of two related finite structures. The first is the Steiner system S(5,8,24), a combinatorial block design. Two independent works by Witt and Carmichael showed that the automorphism group on this structure is isomorphic to the permutation group generated by Mathieu. The second is the extended Golay error-correcting code and is of primary interest to this review paper. The extended Golay code is distinct from the Steiner System in its tangibility and practical applications. This feature makes the Golay code feel tractable and presents a tempting target for reasearchers intersted in constructing M_{24}. In the paper "Build a Sporadic Group in Your Basement", the authors attempt to leverage this by generating a representation for the automorphism on the extended Golay code that is "as simple" as possible." In doing so, they necessarily also generate a natural and enlightening construction for the Mathieu group M_{24}.

Proofs and Results

Building the Sporadic Group M_{24} will require some introductory results and definitions from coding theory. For this discussion, we limit our scope to the algebraic properties of error-correcting codes and omit properties relevant to engineering applications. These properties are interesting but they are not relevant to the construction of M_{24}. We begin with some notation and definitions.

For simplicity, let F denote the field of binary numbers. Define addition and multiplication on this field by

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	0

Figure 1. binary addition and multiplication tables for the field F

Definition 1 (Binary Code)**.** A *Binary Code* with length n is a set of vectors $C = \{c_1, c_2, ..., c_m\}$ where each vector c_i $i = 0, 1, ..., m$, is chosen from F^n. The vectors of this set are called *Codewords*.

It follows from this definition that the set

$$S = \{[0,0,0], [1,0,0], [0,1,0], [1,1,0]\} \tag{1}$$

is a binary code of length 3. The vectors $[0,0,0]$ and $[0,1,0]$ are codewords of S.

The code S also happens to be closed under vector addition and scalar multiplication. In other words, S comprises a subspace of F^3. This property motivates our next definition.

Definition 2 (Linear Binary Code)**.** A *Linear Binary Code* with dimension k is a binary code that completely exhausts a subspace of F^n with dimension k.

Returning to our example, we see that the vectors $[1,0,0]$ and $[0,1,0]$ form a basis for the code S. In particular, S contains all the vectors generated by that basis. Thus, we say S is a linear code with dimension 2.

It is customary to stack basis vectors for a code C as row vectors in a *generator matrix* M. A valid generator matrix for S is

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Note that this generator matrix is not unique.

Next, we address the *minimum distance* for a linear code. The *distance* between two codewords c_1 and c_2, denoted $\text{dist}(c_1, c_2)$, is the number of coordinates in which c_1 and c_2 differ. The *weight* of a codeword c, $\textit{weight}(c)$, is then defined to be $\text{dist}(c, \mathbf{0})$, where $\mathbf{0} = [0, 0, ..., 0]$

remark. Usually, the minimum distance for a binary code C is the minimum value of the set $\{\text{dist}(c_1, c_2) \mid c_1, c_2 \in C\}$. However for this reveiw, we are interested in linear codes. For linear codes, we always have that $\text{dist}(c_1, c_2) = \text{dist}(c_1 + c_2, 0) = \text{dist}(c_3, 0)$ from some $c_3 \in C$. In this case, the minimum distance is just the smallest *weight* of any codeword $c \in C$.

Definition 3 (Minimum Distance)**.** The *Minimum Distance* of a linear binary code is the minimum value of $\{\text{weight}(c) \mid c \in C\}$.

Up to this point, we have defined 3 important paramters of linear codes. These include the *length*, the *dimension*, and the *minimum distance*. We call a linear code with length n, dimension k, and minimum distance d an (n, k, d)-code.

The Golay Code

The extended Golay Code will be instrumental in our construction of M_{24}. It is a linear binary $(24,12,8)$-code that was introduced by Marcel Golay in 1949. It is most easily assembled by the following greedy algorithm:

First, write down the numbers $0,1,2,...,2^{24}-1$ and consider their representations as binary codewords of length 24. We will scan the list one by one and collect the codewords of the extended Golay code. Begin by adding 0 to the collection. This will be the first extended Golay codeword. Now scan the values $1,2,...,2^{n-1}$ and add any value to the collection with distance at least 8 from any of the previously collected codewords. The resulting collection will be the extended Golay code.

The extended Golay code belongs to a special class of linear codes called *self-dual* codes. This property gives us a computationally inexpensive method for recognizing Golay codewords.

Definition 4 (Self-Dual Codes)**.** A linear code C is called *self-dual* if $C = C^{\perp}$, where $C^{\perp} = \{x \mid x \cdot c = 0, \forall c \in C\}$. Note that $c_1 \cdot c_2$ is an inner product defined as the usual dot product modulo 2.

It follows from this definition that the Golay codewords are precisely the words which are orthogonal to any given generator matrix for the Golay code.

Equivalent Codes and Automorphisms

Recall that a homomorphism is a map $f : A \to B$ that preverves an operation defined on the algebraic structures A and B. That is, for some property μ defined on A and B, we have $f(\mu_A(a_1,a_2)) = \mu_B(f(a_1), f(a_2))$ for all $a_1, a_2 \in A$.

We will be interested in homomorphisms on Linear Codes which preserve the distance operation.

Definition 5 (Equivalent Linear Codes)**.** Two Linear Binary Codes C and D of length n are *equivalent* if a coordinate permutation on the codewords of C produces the codewords in D. More precisely, C and D are equivalent if there is a bijective map $\pi : C \to D$ where $\pi(c)$ is a coordinate permutation on the codeword c.

remark. A coordinate permutation $\pi : C \to D$ is a homomorphism which preserves the distance operation. In particular, $\text{dist}(c_1,c_2) = \text{dist}(\pi(c_1), \pi(c_2))$ for all $c_1, c_2 \in C$.

An *Automorphism* is a bijective homomorphism of the form $f : A \to A$. Note that f maps A back onto itself.

Definition 6 (Linear Code Automorphisms)**.** An *Automorphism* on a code C is a coordinate permutation $\pi : C \to C$ which maps the codewords of C back *into* the codewords of C. Such a mapping must be bijective.

Lemma 1. A permutation that maps a basis for a code C to another basis is necessarily an automorphism on C. *(proof omitted)*

Lemma 2. The set of automorphisms on a code C form a group under composition, denoted, Aut(C).

The extended Golay code revisited

We will now explore some properties of the extended Golay code in light of *equivalence* and *automorphisms*. Earlier we mentioned that the extended Golay code is an example of a $(24,12,8)$-code. We will see in the following theorem that any code with this property is equivalent to the extended Golay code.

Theorem 1 (Pless)**.** Let C be a linear binary $(24,12,d)$-code. Then the following statements are equivalent:

1. The minimum weight of C is d.
2. C is equivalent to the extended Golay code.

We also state the following theorem which will serve as our primary tool in constructing a natural representation for M_{24}.

Theorem 2 (Huffman, Pless)**.** The full automorphism group of the extended binary Golay code, denoted Aut(G), is isomorphic to M_{24}.

Theorem 2 has the natural consequence that any subgroup of Aut(G) will be isomorphic to a subgroup of M_{24}. This suggests a clever strategy for constructing M_{24}. If we generate a group by composing two automorphisms of G, then we are gauranteed the resulting subgroup will be isomorphic to a subgroup of M_{24}. Thus we might attempt to build M_{24} by choosing the 'right' pair of automorphisms on G in the hopes that they might exhaust all elements of Aut(G). Such a pair would also generate M_{24}.

Building the Sporadic Group

We now have the necessary vocabulary to disscuss a construction of M_{24}. In fact, we will simply build the group outright.

After developing and expanding on the coding theory which we have just presented, the authors of "Build a Sporadic Group in Your Basement" eventually arrive at the following construction for M_{24}. The result is a subgroup of the symmetric group S_{24} generated by two permutation:

$$\tau = (1,2,3,4,5,15,19,11,10,9,12,7,13,14,23,24,17,18,22,6,21,8,20)(16)$$
$$\rho = (1,2,3)(4,5,6)...(22,23,24)$$

The software package **GAP** was used to verify that the group generated by τ and ρ is simple with 244,823,040 elements. This fact along with the following lemma stated in the paper is illuminating.

Lemma 3. The only simple group of order 244, 823, 040 is the Mathieu group M_{24}.

The group constructed by τ and ρ is the Mathieu group M_{24}. We will now attempt to uncover how the authors arrived at this construction. In doing so, we will also provide an alternate proof that this is M_{24} through the avenue of Theorem 2. In particular, we show that τ and ρ are both automorphisms on the extended Golay code. To this end we introduce two new models of the extended Golay code.

Quadratic Residue Model (R)

The Quadratic Residue model is almost exactly the model originally proposed by Marcel Golay. The generator matrix for the code is produced by the set $\{1,2,3,4,6,8,9,12,13,16,18\}$, the set of numbers q which allow integers solutions to the equation $x^2 \equiv q \pmod{23}$. The first codeword in the generator matrix is the vector with ones in these positions, an additional one in position 24, and the remaining positions zero. The next 11 rows are generated by applying the permutation

$$\sigma = (1,2,3,4,5,15,19,11,10,9,12,7,13,14,23,24,17,18,22,6,21,8,20)(16)$$

to the previously generated row. This yields the generator matrix:

$$Q = \begin{bmatrix}
11110101100110010100000\;1 \\
01111010110011001010000\;1 \\
00111101011001100101000\;1 \\
00011110101100110010100\;1 \\
00001111010110011001010\;1 \\
00000111101011001100101\;1 \\
10000011110101100110010\;1 \\
01000001111010110011001\;1 \\
10100000111101011001100\;1 \\
01010000011110101100110\;1 \\
00101000001111010110011\;1 \\
10010100000111101011001\;1
\end{bmatrix}$$

A moderate amount of python code shows that the permutation σ maps the final row of Q to the vector sum of columns 1,2,3,4,5,8, and 11. This is the only combination of basis codewords in Q which achieves this. Thus σ maps the basis codewords of Q to a new linearly independent basis. By Lemma 1, σ is automorphism on the extended Golay code.

Block-Substitution Model (B)

We now turn our attention to the Block-Substitution model of the Golay code. This model was introduced by the authors of "Build a Sporadic Group in Your Basement." We proceed by substituting the $3x3$ matrix blocks

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \bar{I} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad J = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{into the matrix} \quad G = \begin{bmatrix} I & 0 & 0 & 0 & \bar{I} & I & I & J \\ 0 & I & 0 & 0 & J & \bar{I} & I & I \\ 0 & 0 & I & 0 & I & J & \bar{I} & I \\ 0 & 0 & 0 & I & I & I & J & \bar{I} \end{bmatrix}$$

to obtain

$$
G = \begin{bmatrix}
100000000000011100100111 \\
010000000000101010010111 \\
001000000000110001001111 \\
000100000000111011100100 \\
000010000000111101010010 \\
000001000000111110001001 \\
000000100000100111011100 \\
000000010000010111101010 \\
000000001000001111110001 \\
000000000100100100111011 \\
000000000010010010111101 \\
000000000001001001111110
\end{bmatrix}
$$

Again, we will seek an automorphism that preserves the basis codewords of our generator matrix G. The cyclic structure of the blocks I, $\bar{I}$, and J suggests the permutation

$$\rho = (1,2,3)(4,5,6)...(22,23,24)$$

Indeed, this permutation completely preserves the row vectors of G. Moreover, it is one of the two permutation we saw early which the authors use to build M_{24}.

Taking Stock

We now have two automorphisms, σ and ρ, which operate on distinct Golay code models R and B.

Both of these permutations fell naturally out of their respective Golay code models. The hope presented in BSGYB is that the models R and B might be "different" enough that their corresponding automorphisms would generate the full Golay code automorphism group. We might be tempted to compose these permutations directly to this end. However this approach would be meaningless. σ and ρ operate on distinct codes so they do not preserve any useful structure.

Instead we will seek an equivalence map from B to R. The resulting map can then be used to express σ as an automorphism on the code B. More precisely, for an equivalence map, χ: $B \to R$, and an automorphism σ on R, we are gauranteed that $\chi^{-1}\sigma\chi$ will be an automorphism on B. This follows because $\chi^{-1}\sigma\chi$ is injective and maps codewords of B back into B. Moreover, Theorem 1 promises that this equivalence map exists for our two $(24,12,8)$-code models. It is simply our task to find it.

Bridging the gap from B to R

Finding an equivalence map from B to R is a computationally difficult problem. We're looking for some permutation, χ, which maps each of the 2^{12} codewords of B into some codeword of R. Fortunately, equivalence maps between Golay codes cannot be unique. Any single equivalence map $\kappa : B \to R$ can be combined with a permutation $\beta \in Aut(R)$ so that $\beta\kappa$ is also an equivalence map. Still, we expect valid choices for χ to be sparse.

A brute force approach would require searching the entire space of 24! permutations. Each iteration would test whether a candidate permutation takes the rows of the generator matrix G to words generated by Q. Definition 3 makes this easy since the codewords generated by Q are exactly the words which are orthogonal to Q. However, this added convenience will only be useful once we find a stronger set of constraints to narrow the search space.

We can begin by making a tactical guess. The intersection of our two Golay models, $B \cap R$, contains exactly 4 codewords generated by the basis $\hat{1} = [1,1,...,1]$ and $\hat{z} = [0,1,1,0,0,1,0,0,1,1,0,0,0,0,1,1,1,0,0,1,1,0,1,1]$. The fact that these codewords are contained in both models suggests that χ maps words in $B \cap R$ back to themselves. In particular, we will make the guess that χ fixes $\hat{z}$. This essentially partitions the nonzero coordinates and zero coordinates of $\hat{z}$, given respectively by

$$C = \{2,3,6,9,10,15,16,17,20,21,23,24\},$$
$$D = \{1,4,5,7,8,11,12,13,14,18,19,22\}$$

so that coordinates in C must be sent to C and coordinates in D must be sent to D. This drastically reduces the search space from 24! to $(12!)^2$ possible permutations to consider. This is an improvement but we can do better by observing some properties of the automorphism group on the extended Golay code.

The original construction of the Mathieu group M_{24} is well-known to be a *5-transitive* permutation group. This property gaurantees that for distict elements x_1,x_2,x_3,x_4,x_5 and distinct elements y_1,y_2,y_3,y_4,y_5 chosen from the set $\{1,2,...,24\}$, there is a permutation in M_{24} which takes the ordered tuple (x_1,x_2,x_3,x_4,x_5) to the ordered tuple (y_1,y_2,y_3,y_4,y_5). Theorem 2 tells us that this property also holds for coordinate permutations of the automorphism group of the code R. In particular, we can always find a permutation $\alpha \in Aut(R)$ which takes a given ordered tuple of coordinates (i_1,i_2,i_3,i_4,i_5) to the coordinates $(1,2,3,4,5)$.

This property allows for another simplifying assumption. Earlier we mentioned that an equivalence map $\kappa : B \to R$ can be combined with an automorphism $\beta \in Aut(R)$ to make an equivalence map $\beta\kappa$. We know that κ must exist and β may be selected to send any 5 coordinates to the coordinates $(1,2,3,4,5)$. Thus there is some equivalence map which fixes the first five coordinates. We will guess that χ additionally has this property. This further refines our partition into the three sets:

$$
\begin{aligned}
F &= \{1,2,3,4,5\} \\
C &= \{6,9,10,15,16,17,20,21,23,24\} \\
D &= \{7,8,11,12,13,14,18,19,22\}
\end{aligned}
$$

where F is the fixed coordinates of χ and C and D are disjoint sets which χ maps independently. This is just the result of moving the coordinates $1-5$ from our original C and D to the set of fixed coordinates F. Note that this is consistent with the hypothesis that χ sends $\hat{z}$ to $\hat{z}$.

We would now like a method to systematically deduce the mappings of individual coordinates in C and D. We will find that tools from combinatorics will be helpful. The codewords of minimum weight $d = 8$ of any Golay code form a t - (v,k,λ) combinatorial block design with parameters $t = 5, v = 24, k = 8$ and $\lambda = 1$. For our purposes, this simply means that for a Golay code model, M, and an ordered 5-tuple of coordinates, (i_1,i_2,i_3,i_4,i_5), there is exacly one minimum-weight codeword in M containing all 1s at these positions. We will leverage this by only considering codewords in B and R with minimum weight. It turns out that the subset of minimum weight words always forms a basis for a Golay code. So any permutation which satisfies the minimum weight codewords of B and R will satisfy all codewords. We will then use specific 5-tuples of nonzero coordinates along with information about F,C, and D to anchor words in B to corresponding words in R. Doing this will give us better insights into the mappings of particular coordinates in C and D.

Determining C and D

Let B' and R' denote the respective subsets of the codewords in B and R having minimum weight, $d = 8$. Note that codewords of B' must map to codewords of R' under an equivalence map. We know that there is exactly one codeword in B' starting with five consecutive 1s. If our assumption that χ fixes the coordinates of F is true, then this word must map to the unique codeword in R' starting with five ones. Searching B' and R' for these words yields the mapping:

$$
\begin{aligned}
\chi : &[1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,\mathbf{1},0,0,1,0,0,1] \\
\to &[1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,1,0,\mathbf{1},0,0,1,0,0,0]
\end{aligned}
$$

We've bolded the nonzero coordinates of D for illustrative purposes. If our assumptions up to this point have been correct, then the permutation χ must take the set of nonzero coordinates $\{18,21,24\} \to \{16,18,21\}$. Moreover, coordinates in D must be mapped back to coordinates in D. Thus the mapping $18 \to 18$ is determined. We are uncertain about the exact determination of $\{21,24\} \to \{16,21\}$ however the authors argue that additional fixed points are to be expected. Thus we make another simplifying guess and suppose that 21 is fixed while $24 \to 16$. This new information yields the following updated constraints on our desired equivalence map χ

$$
\begin{aligned}
F &= \{1,2,3,4,5,18,21\} \\
C &= \{6,9,10,15,16,17,20,23,24\} \qquad \chi : 24 \to 16 \\
D &= \{7,8,11,12,13,14,19,22\}
\end{aligned}
$$

Discussion

The Discussion should be succinct and must not contain subheadings.

Methods

Topical subheadings are allowed. Authors must ensure that their Methods section includes adequate experimental and characterization data necessary for others in the field to reproduce their work.

References

1. Hao, Z., AghaKouchak, A., Nakhjiri, N. & Farahmand, A. Global integrated drought monitoring and prediction system (GIDMaPS) data sets. *figshare* http://dx.doi.org/10.6084/m9.figshare.853801 (2014).

LaTeX formats citations and references automatically using the bibliography records in your .bib file, which you can edit via the project menu. Use the cite command for an inline citation, e.g.[1].

For data citations of datasets uploaded to e.g. *figshare*, please use the `howpublished` option in the bib entry to specify the platform and the link, as in the `Hao:gidmaps:2014` example in the sample bibliography file.

Acknowledgements (not compulsory)

Acknowledgements should be brief, and should not include thanks to anonymous referees and editors, or effusive comments. Grant or contribution numbers may be acknowledged.

Author contributions statement

Must include all authors, identified by initials, for example: A.A. conceived the experiment(s), A.A. and B.A. conducted the experiment(s), C.A. and D.A. analysed the results. All authors reviewed the manuscript.

Additional information

To include, in this order: **Accession codes** (where applicable); **Competing interests** (mandatory statement).

The corresponding author is responsible for submitting a competing interests statement on behalf of all authors of the paper. This statement must be included in the submitted article file.

Figure 2. Legend (350 words max). Example legend text.

Figures and tables can be referenced in LaTeX using the ref command, e.g. Figure 2 and Table 1.

Condition	n	p
A	5	0.1
B	10	0.01

Table 1. Legend (350 words max). Example legend text.