The Mathieu Groups

Stephen Zhou

July 2025

Introduction

Theorem (Jordan-Holder)

Let G be a group. Then G has a composition series; that is, a sequence

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1, \tag{1}$$

where G_i/G_{i+1} is a simple group for all i. Moreover, the composition factors G_i/G_{i+1} are unique up to isomorphism and ordering.

Introduction

Theorem (Classification of FSG's)

Any finite simple group is either:
i) Cyclic or alternating,
ii) Contained in one of 16 *infinite families of groups, collectively known as the groups of Lie type*
ii) One of 26 *other sporadic groups.*

- VERY hard proof
- 10,000+ pages by 100+ authors over decades
- Correcting the proof took decades more
- Being compiled into a book
- Classification is sometimes necessary to prove things.

Sporadic Groups

- Sporadic groups are weird
- $\mathcal{M}_{24}, \mathcal{M}_{23}, \mathcal{M}_{22}, \mathcal{M}_{12}, \mathcal{M}_{11}$
- First sporadic groups

Sporadic Groups

- Sporadic groups are weird
- $\mathcal{M}_{24}, \mathcal{M}_{23}, \mathcal{M}_{22}, \mathcal{M}_{12}, \mathcal{M}_{11}$
- First sporadic groups
- ONLY known sporadic groups for 100 years

Sporadic Groups

- Sporadic groups are weird
- $\mathcal{M}_{24}, \mathcal{M}_{23}, \mathcal{M}_{22}, \mathcal{M}_{12}, \mathcal{M}_{11}$
- First sporadic groups
- ONLY known sporadic groups for 100 years
- Mathieu discovered them

Sporadic Groups

- Sporadic groups are weird
- $\mathcal{M}_{24}, \mathcal{M}_{23}, \mathcal{M}_{22}, \mathcal{M}_{12}, \mathcal{M}_{11}$
- First sporadic groups
- ONLY known sporadic groups for 100 years
- Mathieu discovered them
- Carmichael proved they exist

Sporadic Groups

- Sporadic groups are weird
- $\mathcal{M}_{24}, \mathcal{M}_{23}, \mathcal{M}_{22}, \mathcal{M}_{12}, \mathcal{M}_{11}$
- First sporadic groups
- ONLY known sporadic groups for 100 years
- Mathieu discovered them
- Carmichael proved they exist
- Conway found Conway groups $\mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3$.

Sporadic Groups

- Sporadic groups are weird
- $\mathcal{M}_{24}, \mathcal{M}_{23}, \mathcal{M}_{22}, \mathcal{M}_{12}, \mathcal{M}_{11}$
- First sporadic groups
- ONLY known sporadic groups for 100 years
- Mathieu discovered them
- Carmichael proved they exist
- Conway found Conway groups $\mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3$.
- Golay code construction

Codes

- Say we send a message of bits through a noisy channel
- i.e Computers

Codes

- Say we send a message of bits through a noisy channel
- i.e Computers
- How to 'pad' bits

Codes

- Say we send a message of bits through a noisy channel
- i.e Computers
- How to 'pad' bits
- For example, consider the code we get by repeating every bit 3 times
- 110 can be corrected into 111

Codes

We need symmetry to get nice groups

Definition

A linear code C is a subspace of $\mathbb{F}_2^n$. A matrix whose rows span C is called a generating matrix of C.

Example

The n-repetition code $C = \{(0, \ldots, 0), (1, \ldots, 1)\}$ over $\mathbb{F}_2^n$ is the linear code with generator matrix $[1\,1\ldots1]$.

Codes

- Hamming distance $=$ # of differing bits
- We call an code with dimension k and minimal hamming distance d an $[n, k, d]$ code.
- How many errors can we correct?

Codes

- Hamming distance $=\#$ of differing bits
- We call an code with dimension k and minimal hamming distance d an $[n, k, d]$ code.
- How many errors can we correct?
- $\lfloor \frac{d-1}{2} \rfloor$ errors corrected, where d is minimal hamming distance between codewords
- "Hamming spheres" of radius $\lfloor \frac{d-1}{2} \rfloor$ must not overlap

Example

The n repetition code is a $[n, 1, n]$ code.

Codes

A more complicated example:

Example

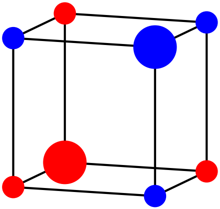
The $(7,4)$ *Hamming code is the* $[7,4,3]_2$ *code with generator matrix*

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{2}$$

- Weight $=$ number of ones
- Notice that the minimal distance between two points of a linear code is the minimal weight of a code
- Proof: Just add!
- We can just check minimal weight by hand.

Perfect Codes

- A perfect code = no "wasted space".
- Every vector is within $(d-1)/2$ of exactly one codeword
- i.e Hamming spheres partition the space
- All the codes we have shown are perfect



The Hamming Bound

Theorem

If there exists a $[n, k, d]$ perfect binary code, then

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{(d-1)/2} = 2^{n-k} \tag{3}$$

Just count the points in each "Hamming sphere".

Perfect Codes

- $n = d$, trivial
- $n = (d-1)/2$, odd repetition codes
- $\binom{2^k-1}{0} + \binom{2^k-1}{1} = 2^k$, Hamming codes

We have only found two more examples:

$$\binom{90}{0} + \binom{90}{1} + \binom{90}{2} = 2^{12} \tag{4}$$

and

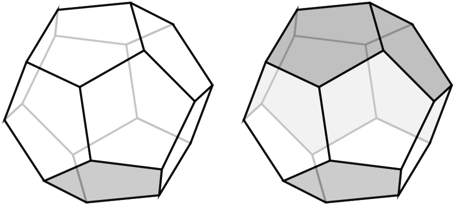
$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}. \tag{5}$$

The $n = 90, d = 5$ case doesn't correspond to a code.

The Golay code

- The $n = 23, d = 7$ case: Golay code G_{23}.

- The $n = 23, d = 7$ case: Golay code G_{23}.
- We will construct this by first defining the extended Golay code G_{24}, and then deleting a bit from it.
- Info bit + padding bit on separate dodecahedrons.
- Info bits are whatever message we want to send
- Padding bits are sum of info bits on nonadjacent faces.



The Golay code

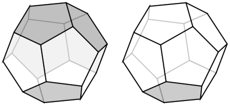
Theorem

The minimal weight of G_{24} is 8.

Lemma

If $\mathbf{a} = (a_1, \ldots, a_{12}, \ldots, a_{24}) \in G_{24}$*, then* $\mathbf{a}' = (a_{13}, a_{14}, \ldots, a_1, a_2, \ldots, a_{12}) \in G_{24}$.

Proof.



We only need to check this on generators. □

- Since G_{24} is a $[8, 12, 24]$ code, G_{23} is a $[7, 12, 23]$ code.

The Mathieu Groups

- $\mathcal{M}_{24}$ is the set of permutations fixing G_{24}
- We view this group as acting on $X = \{1, 2, \ldots, 24\}$
- Other Mathieu groups are defined as stabilizer subgroups

Definition

A group G is said to act on X k-transitively if for any $a_1, a_2, \ldots, a_k \in X$ and $b_1, b_2, \ldots, b_k \in X$, there exists $g \in G$ such that $a_i \cdot g = b_i$.

Example

S_n acts on $\{1, 2, \ldots, n\}$ n-transitively
A_n acts on $\{1, 2, \ldots, n\}$ $n - 2$ transitively

k-transitivity

- The Mathieu groups turn out be be k-transitive for large k
- $\mathcal{M}_{24}$ acting on 24 points is 5-transitive
- $\mathcal{M}_{12}$ acting on 12 points is 5-transitive
- $\mathcal{M}_{23}$ acting on 23 points in 4-transitive
- $\mathcal{M}_{11}$ acting on 11 points in 4-transitive
- $\mathcal{M}_{22}$ acting on 22 points in 3-transitive

k-transitivity

- The Mathieu groups turn out be be k-transitive for large k
- $\mathcal{M}_{24}$ acting on 24 points is 5-transitive
- $\mathcal{M}_{12}$ acting on 12 points is 5-transitive
- $\mathcal{M}_{23}$ acting on 23 points in 4-transitive
- $\mathcal{M}_{11}$ acting on 11 points in 4-transitive
- $\mathcal{M}_{22}$ acting on 22 points in 3-transitive
- Aside from S_n and A_n, no groups of transitivity ≥ 5 exist
- The only 5-transitive groups are $\mathcal{M}_{24}, \mathcal{M}_{12}, S_n, A_n$
- The proof relies on the classification!

Thanks

Thank you for your attention! Any questions?