Review: Build a Sporadic Group in Your Basement

Parker Hyde

Georgia State University

March 1, 2022

What is a Group?

What is a Group?

- $(G, *)$

What is a Group?

- $(G, *)$
- satisfying the properties:
  1. closure $a, b \in G \implies a * b \in G$
  2. associativity: $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$
  3. existence of identity: $\exists e \in G$ s.t. $a * e = e * a = a \; \forall a \in G$
  4. existence of inverses: $\forall a \in G, \exists a^{-1}$ s.t. $a * a^{-1} = a^{-1} * a = e$

What is a Group?

- $(G, *)$
- satisfying the properties:
  1. closure $a, b \in G \implies a * b \in G$
  2. associativity: $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$
  3. existence of identity: $\exists e \in G$ s.t. $a * e = e * a = a \ \forall a \in G$
  4. existence of inverses: $\forall a \in G, \exists a^{-1}$ s.t. $a * a^{-1} = a^{-1} * a = e$

Examples: $(\mathbb{Z}, +)$

What is the Sporadic group M_{24}?

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ)$

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$
- $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$
- $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$

- A Sporadic Group is a *special* of finite simple group.

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$
- $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$

- A Sporadic Group is a *special* of finite simple group.
- A simple group is a group with no nontrivial normal groups.

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$
- $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$

- A Sporadic Group is a *special* of finite simple group.
- A simple group is a group with no nontrivial normal groups.

Example

- $5\mathbb{Z} = \{..., -10, -5, 0, 5, 10, ...\} \trianglelefteq \mathbb{Z}$

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$
- $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$

- A Sporadic Group is a *special* of finite simple group.
- A simple group is a group with no nontrivial normal groups.

Example

- $5\mathbb{Z} = \{..., -10, -5, 0, 5, 10, ...\} \trianglelefteq \mathbb{Z}$
- $\implies \frac{\mathbb{Z}}{5\mathbb{Z}} = \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

What is the Sporadic group M_{24}?

- $M_{24} \leq S_{24} = (\pi_{24}, \circ) \ni \begin{pmatrix} 1 & 2 & 3 & \cdots & 23 & 24 \\ 2 & 3 & 4 & \cdots & 24 & 1 \end{pmatrix}$
- $|M_{24}| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$

- A Sporadic Group is a *special* of finite simple group.
- A simple group is a group with no nontrivial normal groups.

Example

- $5\mathbb{Z} = \{..., -10, -5, 0, 5, 10, ...\} \trianglelefteq \mathbb{Z}$
- $\implies \frac{\mathbb{Z}}{5\mathbb{Z}} = \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

- M_{24} is an unusual finite simple group.

Mathieu's Construction

- M_{24} was originally constructed by the following three arbitrary permutations.

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

Mathieu's Construction

- M_{24} was originally constructed by the following three arbitrary permutations.

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

- link: http://www.netlify/app.sdfjewhwef.com

The Extended Golay Code

The Extended Golay Code

- First, write down the numbers $0,\ 1,\ 2,\ \ldots,\ 2^{24}-1$.

The Extended Golay Code

- First, write down the numbers $0,\ 1,\ 2,\ \ldots,\ 2^{24}-1$.
- Consider their binary representation as 24-bit words.

The Extended Golay Code

- First, write down the numbers $0, 1, 2, \ldots, 2^{24} - 1$.
- Consider their binary representation as 24-bit words.
- Add 0 to the list.
-

$$000000000000000000000000$$

The Extended Golay Code

- First, write down the numbers 0, 1, 2, ..., $2^{24}-1$.
- Consider their binary representation as 24-bit words.
- Add 0 to the list.
- Add any number differing in at 8 bit positions from previously added words.
-

$$000000000000000000000000$$
$$000000000000000011111111$$

The Extended Golay Code

- First, write down the numbers 0, 1, 2, ..., $2^{24} - 1$.
- Consider their binary representation as 24-bit words.
- Add 0 to the list.
- Add any number differing in at 8 bit positions from previously added words.
- Which gives an extended Golay Code:
-

$$
\begin{array}{c}
000000000000000000000000 \\
000000000000000011111111 \\
000000000000111100001111 \\
000000000011001100110011 \\
000000000101010101010101 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}
$$

Two Extended Golay Code Models

Quadratic Residue (R)

$$
\begin{bmatrix}
111101011001100101000001 \\
011110101100110010100001 \\
001111010110011001010001 \\
000111101011001100101001 \\
000011110101100110010101 \\
000001111010110011001011 \\
100000111101011001100101 \\
010000011110101100110011 \\
101000001111010110011001 \\
010100000111101011001101 \\
001010000011110101100111 \\
100101000001111010110011
\end{bmatrix}
$$

Block-Substitution (B)

$$
I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad
\bar{I} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad
J = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}
$$

$$
B = \begin{bmatrix}
I & 0 & 0 & 0 & \bar{I} & I & I & J \\
0 & I & 0 & 0 & J & \bar{I} & I & I \\
0 & 0 & I & 0 & I & J & \bar{I} & I \\
0 & 0 & 0 & I & I & I & J & \bar{I}
\end{bmatrix}
$$

Two Extended Golay Code Models

Quadratic Residue (R)

$$\begin{bmatrix}
111101011001100101000001\\
011110101100110010100001\\
001111010110011001010001\\
000111101011001100101001\\
000011110101100110010101\\
000001111010110011001011\\
100000111101011001100101\\
010000011110101100110011\\
101000001111010110011001\\
010100000111101011001101\\
001010000011110101100111\\
100101000001111010110011
\end{bmatrix}$$

Block-Substitution (B)

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \bar{I} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad J = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} I & 0 & 0 & 0 & \bar{I} & I & I & J \\ 0 & I & 0 & 0 & J & \bar{I} & I & I \\ 0 & 0 & I & 0 & I & J & \bar{I} & I \\ 0 & 0 & 0 & I & I & I & J & \bar{I} \end{bmatrix}$$

$$\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 \ldots, 22, 23)(24)$$

Two Extended Golay Code Models

Quadratic Residue (R)

$$
\begin{bmatrix}
111101011001100101000001\\
011110101100110010100001\\
001111010110011001010001\\
000111101011001100101001\\
000011110101100110010101\\
000001111010110011001011\\
100000111101011001100101\\
010000011110101100110011\\
101000001111010110011001\\
010100000111101011001101\\
001010000011110101100111\\
100101000001111010110011
\end{bmatrix}
$$

Block-Substitution (B)

$$
I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad
\bar{I} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad
J = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}
$$

$$
B = \begin{bmatrix}
I & 0 & 0 & 0 & \bar{I} & I & I & J \\
0 & I & 0 & 0 & J & \bar{I} & I & I \\
0 & 0 & I & 0 & I & J & \bar{I} & I \\
0 & 0 & 0 & I & I & I & J & \bar{I}
\end{bmatrix}
$$

$$\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14..., 22, 23)(24)$$

$$\rho = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)...(22, 23, 24)$$