The Miracle Octad Generator

Mathijs Dingemans

March 28, 2025

1 Introduction

Simple groups are among some of the most important classes of groups, since all finite groups can be written as a semidirect product of simple groups. The simple groups can mostly be classified into 18 different families, such as the cyclic groups of prime order and the alternating groups A_n where $n \geq 5$. However, apart from these 18 families, there are exactly 26 groups that cannot be classified in this way. These groups are called "sporadic groups" and they are among the most interesting groups in the field.

In this paper, we will discuss a method to construct one of these 26 sporadic groups, the Mathieu group M_{24}. This group has a very special connection to one specific code in coding theory, namely the extended binary Golay code (which we will refer to as G_{24} from now on). We will specify exactly how these two objects are related, and how we can use G_{24} to gain some insight into the structure of M_{24}. To this aim, we will define a very special object called the "Miracle Octad Generator", which was first discovered by Rob Curtis in 1976.

2 Steiner Systems

Definition 1. A Steiner $S(t, b, n)$-system with $1 < t < b < n$ is a pair $(\mathcal{S}, \mathcal{B})$, where:

- $\mathcal{S}$ is a set of n elements.
- $\mathcal{B}$ is a collection of subsets of $\mathcal{S}$, called blocks, each of size b.
- Every subset of $\mathcal{S}$ with t elements, is contained in exactly one block.

The third condition, together with the second condition, fix the amount of blocks that we have in our subset. For example, in Steiner system $S(2, 3, 7)$, the subsets $\{1, 2, 3\}$ and $\{1, 2, 4\}$ cannot both be valid blocks, since the subset $\{1, 2\}$ with 2 elements is contained in both blocks.

Example 1. A common example of a Steiner system, is the Fano plane. The plane corresponds with the Steiner system $S(2, 3, 7)$, where the points on the plane are the elements of the set, and every line corresponds to a block. Through every 2 points, there is exactly one line, so the third condition is satisfied and we have a valid Steiner system.

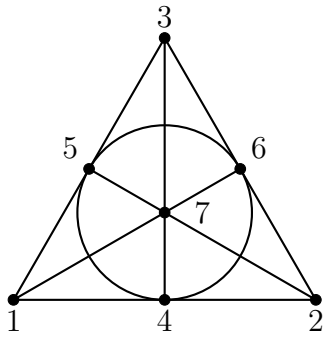


Figure 1: The Fano Plane

To be exact, we have :

$$\mathcal{S} = \{1, \ldots, 7\}$$
$$\mathcal{B} = \{\{1, 2, 4\}, \{1, 3, 5\}, \{1, 6, 7\}, \{2, 3, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{4, 5, 6\}\}$$

And every subset of 2 elements is contained in exactly one of the seven blocks, so the third condition is satisfied.

Lemma 1. *A Steiner $S(t, b, n)$-system has exactly $\frac{\binom{n}{t}}{\binom{b}{t}}$ blocks.*

Proof. We will show this, by counting the amount of subsets of $\mathcal{S}$ with t elements. By definition, there are $\binom{n}{t}$ of these subsets in total. However, since every subset is also contained in exactly one block of size b, we get that the total amount of t-subsets is also equal to $B * \binom{b}{t}$, where B is the amount of blocks. Since both expressions are equal to each other, we get:

$$B = \frac{\binom{n}{t}}{\binom{b}{t}}.$$

□

Remark 1. It is important to note that for some choices of t, b and n, the system $S(t, b, n)$ does not exist. We have seen that $S(2, 3, 7)$ is a valid system, but $S(2, 3, 8)$ is not for example. From Lemma 1, we get that there are $\frac{n(n-1)}{6}$ total blocks when $t = 2$ and $b = 3$, so for any existing Steiner system with these parameters, $n(n-1)$ has to be divisible by 6. This is the case when $n = 7$, but not when $n = 8$, so $S(2, 3, 8)$ cannot be an existing system. The uniqueness of some Steiner system is also not a trivial question. As an example, $S(2, 3, 7)$ is unique up to isomorphism, but there are 2 different systems $S(2, 3, 13)$.

The definition of the Mathieu group M_{24} is that it is the automorphism group of the (unique) Steiner system $S(5, 8, 24)$. From here, we will give a specific construction of $S(5, 8, 24)$ and prove that this construction is in fact a Steiner system.

3 The extended binary Golay code G_{24}

Definition 2. A **linear code** C of length m and dimension r, is an r-dimensional subspace of $\mathbb{F}_q^m$, for which any linear combination of codewords, is an element of the code itself.
In other words:

$$\forall a, b \in \mathbb{F}_q, \forall \mathbf{x}, \mathbf{y} \in C : a\mathbf{x} + b\mathbf{y} \in C$$

In this part, we will only work with codes where $q = 2$, which we call binary codes.

Definition 3. We call a matrix G the **generatormatrix** of a linear code C, if the rows of this matrix span the entire code.

Definition 4.

- The **Hamming distance between two codewords** is the number of elements where the two codewords differ. (e.g. $d(01010, 00100) = 3$)
- The **Hamming distance of code** C is the smallest possible distance between two different codewords. (e.g. $d(C) = 3$)

Definition 5. Let B be the 12×12 matrix over $\mathbb{F}_2$:

$$B := \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The extended Golay code G_{24} is the binary code with generator matrix

$$G := [\mathbb{I}_{12} B]$$

Next, we will state two important properties of G_{24}:

Lemma 2.

- *G_{24} is a 12-dimensional subspace of $\mathbb{F}_2^{24}$ and contains 4096 codewords.*
- *Every codeword in G_{24} has one of 5 possible weights: $0, 8, 12, 16$ or 24. These are distributed in the following way:*

weight	*number of codewords*
0	*1*
8	*759*
12	*2576*
16	*759*
24	*1*

We will call the codewords with a weight of 8 "octads". These codewords are the ones we will mostly consider from now on. Note that the entire Golay code is generated by the octads, since all of the first 11 codewords in the generator matrix are octads, and adding the first codeword to the 12th codeword gives us an octad as well which is linearly independant from the other 11 octads.

4 The hexacode $\mathcal{C}_6$

Let $\mathbb{F}_4 \simeq \frac{\mathbb{F}_2[x]}{x^2+x+1}$ be the Galois field with elements $\{0, 1, \omega, \overline{\omega}\}$ where we can identify $\{1, \omega, \overline{\omega}\}$ as the 3rd roots of unity, since:

$$1 + \omega = \overline{\omega}, \qquad 1 + \overline{\omega} = \omega, \qquad \omega + \overline{\omega} = 1 = \omega\overline{\omega}$$

and

$$\omega^2 = \overline{\omega}, \qquad \overline{\omega}^2 = \omega, \qquad \omega^3 = 1 = \overline{\omega}^3.$$

Definition 6. We define the hexacode $\mathcal{C}_6$ as a 3-dimensional subspace of $\mathbb{F}_4^6$. We state the following equivalent definitions:

- $\mathcal{C}_6$ is the subspace generated by the vectors

$$\omega\overline{\omega}\omega\overline{\omega}\omega\overline{\omega}, \quad \omega\overline{\omega}\overline{\omega}\omega\overline{\omega}\omega, \quad \overline{\omega}\omega\omega\overline{\omega}\overline{\omega}\omega, \quad \overline{\omega}\omega\overline{\omega}\omega\omega\overline{\omega}.$$

- Let $w(\phi) = abcdef$ be some word in $\mathbb{F}_4^6$ with $\phi(x) = ax^2 + bx + c$, then $w \in \mathcal{C}_6$ if:

$$\phi(0) = c, \quad \phi(1) = d, \quad \phi(\omega) = e, \quad \phi(\overline{\omega}) = f.$$

This second definition gives rise to a third (very useful) characterization of the hexacode.

Lemma 3. *A vector $abcdef \in \mathcal{C}_6$ if and only if it satisfies the following:*

- *(1-rule) $a + b = c + d = e + f = s$ (where we call s the "slope")*
- *(ω-rule) $a + c + e = a + d + f = b + c + f = b + d + e = \omega s$*
- *($\overline{\omega}$-rule) $b + d + f = b + c + e = a + d + e = a + c + f = \overline{\omega} s$*

This characterization lets us solve the following two problems.

Proposition 1 (The 3-problem)**.** *Given any codeword in $\mathcal{C}_6$ with only 3 given digits, we can find the entire (unique) codeword.*

Proof. We split in two cases:

- If the 3 given digits are all from distinct pairs which complete the 1-rule, then we can deduce the slope s by either the ω or $\overline{\omega}$-rule. With s, we can use the 1-rule to complete all digits.

- If we have a pair between the 3 digits, we can calculate the slope s from that pair and calculate a 4th digit from the pair with the remaining digit. To find the last two digits, use both the ω and $\overline{\omega}$-rule.

□

Proposition 2 (The 5-problem)**.** *Given any codeword in $\mathcal{C}_6$ with 5 given digits where one of the digits might be wrong, we can find the entire codeword.*

Proof. We have 3 pairs in our codeword, and by eliminating one of these pairs, we end up with at least 3 given digits. Since the wrong digit has to be in one of the pairs, we just solve 3 distinct 3-problems, and one of them will result in the correct word with at most 1 deviation. □

Example 2. 3-problem on $\omega?1?0?$:
(ω-rule): $a + c + e = \overline{\omega} = \omega s$, so $s = \omega$. Hence, $b = 0$, $d = \overline{\omega}$ and $f = \omega$.

Example 3. 5-problem on $\omega 10\omega 1?$:
Suppose the last pair is wrong, then $s = \omega + 1 = 0 + \omega$, which is a contradiction.

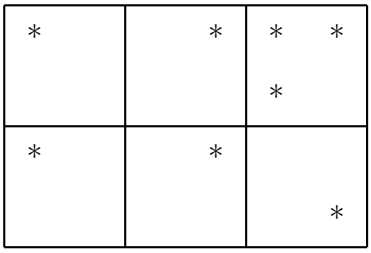
If the second pair is wrong, then $s = \omega + 1 = \overline{\omega}$, and $f = \omega$. Also, $a+c+e = 1$, so $c = \omega$ and hence $d = \overline{\omega}$, which is a contradiction again.

Hence, the first pair has to be wrong, $s = 0 + \omega = \omega$ and $f = \overline{\omega}$. Using again that $a + c + e = \overline{\omega}$, we get that $a = \omega$ and $b = 0$.

5 The Miracle Octad Generator (MOG)

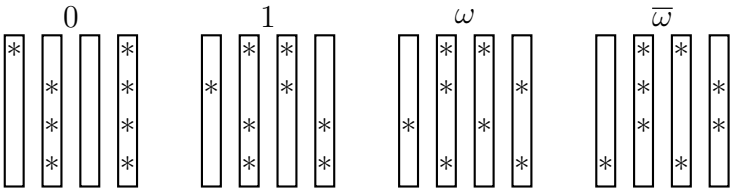
Definition 7. The Miracle Octad Generator (MOG) is a 4×6 array of stars, where the top row and all columns share the same parity: each containing either an odd or even number of stars.

Example 4. This is an example of a MOG-position, since there are either 0 or 2 stars in every column, and 4 stars in the top row.



We also define a function that we can apply to any column of some MOG-position which we will call the score.

Definition 8. There are 16 possible columns that can fill the MOG, we associate every column to some element in $\mathbb{F}_4$ called "the score" in the following way:

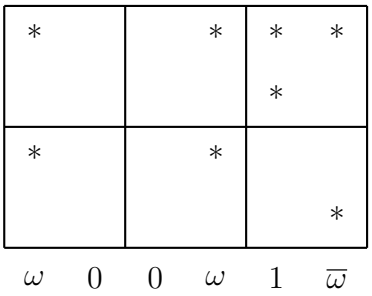


Let columns with an odd number of stars be odd representations and those with an even number be even representations. Each element has 2 odd and 2 even representations.

Definition 9. The extended binary Golay Code G_{24} is the set of all MOG-positions such that the concatenation of the scores of all 6 columns forms a codeword in the hexacode $\mathcal{C}_6$.

The justification as to why we can call this set the Golay code will come later. For now, we just assume this construction is different as the Golay code described in an earlier section.

Example 5. The following MOG-position is an element of G_{24} since $\omega 00\omega 1\overline{\omega} \in \mathcal{C}_6$:



We call the elements of G_{24} that have 8 stars the octads.

Theorem 1. *The octads in G_{24} form a Steiner system $S(5, 8, 24)$.*

Proof. Suppose we have some 4×6 grid with 5 stars, then the column distributions of the columns must be one of the following:

$$410000, \quad 320000, \quad 311000, \quad 221000, \quad 211100, \quad 111110$$

By considering the parity of the columns in all of these cases, we can summarize. Either we have 5 columns of the same parity (and one not), or we have 3 columns of even parity, and 3 columns of odd parity.

- **5 columns of same parity:**
  Every columns has to have the same parity by MOG rules, so we have to change the parity of the 6th column as well, which means we have to add at least 1 star in that column. Since parity has to be preserved, we have to add both of the remaining stars in the same column.

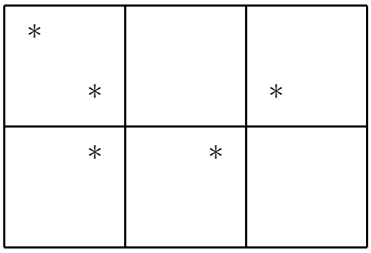
  If we consider the scores of all 6 columns, we have the 5 columns of which we know that at most 1 column is changed, and our unknown column. Hence, we can solve a 5-problem on the score and add the 3 extra stars to get the representations that we need!

- **3 columns even, 3 columns odd**:
  Since every column has to have the same parity, we already know that we have to make changes in 3 columns of the same parity. Looking at the scores again, we have two possible options. Either the scores of the

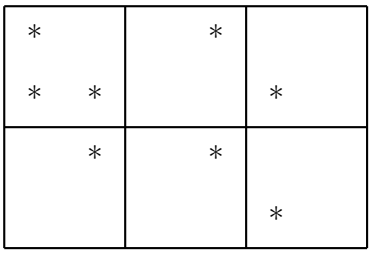
even representations are correct and we have to solve a 3-problem, or the scores of the odd representations are correct and we also have to solve a 3-problem. Only one of these will result in the correct octad.

□

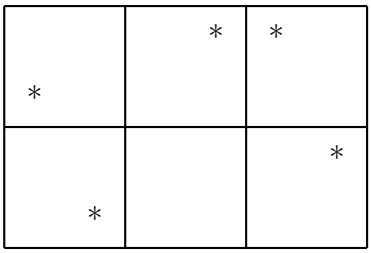
Example 6. For a 3,3 case, consider the following MOG-position:



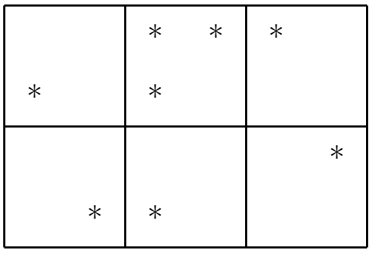
This gives us 2 different 3-problems to solve, namely $0??1\omega?$ and $?\overline{\omega}0??0$. Solving the first 3-problem, we get $0101\omega\overline{\omega}$, which is impossible as we cannot get 1 on the second row. The second 3-problem gives us $1\overline{\omega}0\omega\omega0$, which results in:



Example 7. For a 5 columns having the same parity case, consider the following MOG-position:



We have to solve a 5-problem on $1\overline{\omega}?00\omega$. Solving it, we get that $s = \omega$. We also find that there are no errors, and the decoded word is $1\overline{\omega}\omega00\omega$. This results in the following MOG-position:



Note that this proof is actually fully constructive! If we have any 4×6 grid, with 5 stars given, we can find the exact octad in which the same 5 stars are present by just applying some algorithm. This is one of the reasons why the MOG is such a useful tool for this specific Steiner system.

Finally as promised, we can link the two definitions of the Golay code together by considering the following 4×6 grid:

0	∞	1	11	2	22
19	3	20	4	10	18
15	6	14	16	17	8
5	9	21	13	7	12

If we have some MOG-position that is an element of G_{24}, then its stars will correspond to some numbers on this grid. If we then consider the subset which contains all of these numbers, this subset will be associated to some element of the classical Golay code as described in chapter 3.

References

[1] L. Le Bruyn, *Simple Groups*, Master's Course 2021/2022, Universiteit Antwerpen, 2022.

[2] R. T. Curtis, (1976), *A new combinatorial approach to M24*, Mathematical Proceedings of the Cambridge Philosophical Society, 79 (1): 25–42

[3] T. Chen, (2021), *The Leech Lattice: Sphere packings and the Conway groups*, `https://studenttheses.universiteitleiden.nl/handle/1887/4171249`, 10-36