EULER CIRCLE PAPER: SPORADIC GROUPS

MEHANA ELLIS

ABSTRACT. For my paper, I hope to cover some of the interesting properties of the Conway groups. In particular, the Conway groups are the three sporadic simple groups Co_1, Co_2 and Co_3 (and the related group Co_0). Conway recently passed away, and it seems fitting to write a paper about some of his greatest work.

1. Introduction to sporadic groups

We begin our study of sporadic groups by recalling a few things we've learnt about simple groups.

Definition 1.1. A group G is called *simple* if its only normal subgroups are G and $\{e\}$.

A natural question we ask is whether there is some way to classify the finite simple groups. There is, and this is called the classification theorem.

Theorem 1.2. *The finite simple groups consist of 18 countably infinite families as well as* 26 *sporadic groups that do not fall into any infinite family.*

Essentially, the sporadic groups are exceptions in that they do not fit the pattern of the other 18. Now let's define the three Conway groups:

Definition 1.3. The Conway group Co_1 is a sporadic simple group with order

$$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 4157776806543360000.$$

The Conway group Co_2 is a sporadic simple group with order

$$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 42305421312000.$$

The Conway group Co_3 is a sporadic simple group with order

$$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 495766656000.$$

[CK09]

Date: June 7, 2020.

The largest of the three Conway groups is Co_1. In order to investigate the most interesting facts about these groups, we must learn a few more things.

2. Unimodular lattices & the Leech lattice

Let's look at some prerequisite definitions.

Definition 2.1. A *unimodular* lattice is an integral lattice with determinant either -1 or 1.

Building up from the latter definition, we can introduce the Leech lattice, which we'll be using in our study of the Conway groups.

Definition 2.2. The *Leech lattice* is an even, unimodular lattice which is 24-dimensional. It is commonly denoted as Λ_{24}. [Bor99]

There is a proof that the Leech lattice is unique. Before we prove this, we need to give a few more definitions.

Definition 2.3. A *definite quadratic form* is a quadratic form (polynomial with all terms having degree 2) over a real vector space (call it V) such that for each non-zero vector of V, the quadratic form always has the same sign.

Following from this, we can describe a unimodular lattice called the Neimeier lattice as well as a Lorentzian lattice.

Definition 2.4. There are 24 positive-definite (having the same sign as mentioned in Definition 2.3) even unimodular lattices with rank[1] 24. These are called *Neimeier lattices.* There is also an even 26-dimensional Lorentzian unimodular lattice. This is called the *Lorentzian lattice*, and is denoted $II_{25,1}$. [Bor99]

Now that we have those definitions covered, let's prove that the Leech lattice is unique.

Theorem 2.5. *The Leech lattice is unique.*

Proof. This is equivalent to proving that, given two Neimeier lattices, they are isomorphic if each doesn't have any roots. We essentially want to show that two norm[2] 0 primitive vectors of $II_{25,1}$ are conjugate under $\mathrm{Aut}(II_{25,1})$. If D is a fundamental domain (as in Borcherds's paper) and only has one vector like this, then the Leech lattice is unique. The vector in D is unique, because the roots of D generate the Lorentzian lattice $II_{25,1}$. [Bor99] □

[1] i.e., cardinality maximal linearly independent subset

[2] The norm essentially means the square of the distance from the origin of a vector when we embed the Leech lattice into $\mathbb{R}^{24}$.

There are some more interesting things related to the Leech lattice that we can look at.

Lemma 2.6. *A* 26*-dimensional unimodular lattice* L *with no vectors of norm* 1 *has a characteristic vector of norm* 10*.* [Bor99]

In order to use this Lemma for another proof, we'll need some more definitions:

Definition 2.7. Let V be a vector space over F with bilinear form[3] B. Let u be left-orthogonal to v, and let v be right-orthogonal to u when $B(u, v) = 0$ (a matrix A is said to be left/right-orthogonal if we have $A^K A = I$ or $AA^K = I$). If W is a subset of V, the *left-orthogonal complement* $W^{\perp}$ is

$$W^{\perp} = \{x \in V : B(x, y) = 0 \text{ for all } y \in W\}.$$

Definition 2.8. Loosely speaking, the *Weyl group* is a subgroup of the isometry group of the root system[4]. The hyperplanes that are orthogonal to these roots divide $A \otimes R$ [5] into regions. These regions are called *Weyl chambers.*

Next, let's see another lemma; note that the *type* of vector is the smallest inner product of the vector with a norm 0 vector of $II_{25,1}$.

Lemma 2.9. *The lattice* L *(as defined in Lemma 2.6) has no roots iff* $u^{\perp}$ *has no roots and* u *has type at least* 5*.* [Bor99]

Proof. Note that L must have roots if $u^{\perp}$ has roots. It can be shown (with mild difficulty and several other definitions) that if u has type at most 4, then L has roots. Also, if L has some root a and contains $u^{\perp} + c$ for some c, then either of the following could be the case: (1) a has norm 2 and inner product $0, \pm 2, \pm 4$ with c, or (2) a has norm 1 and inner product $\pm 1, \pm 3$ with c. Either way, $u^{\perp}$ has roots, or u has type at most 4. □

In Borcherds's paper, there are two other lemmas (Lemma 5.5.4 and Lemma 5.5.5), but we will assume their statements, as they are a bit more challenging.

Theorem 2.10. *There exists a unique* 26*-dimensional unimodular lattice* L *with no roots. Its automorphism group acts transitively on the*

[3] A bilinear form can be thought of as a bilinear map $V \times V \to S$, with S being the field of scalars

[4] Think of the root system as a configuration of vectors in Euclidean space.

[5] Tensor product. Essentially, we have a lattice, which is isomorphic to $\mathbb{Z}^n$. The tensor product with R is R^n (with the same basis).

624 *characteristic norm* 10 *vectors of* L *and the stabilizer of such a vector (call it* V*) has order* $5^3 \cdot 2 \cdot 120$. *The automorphism group has order* $2^8 \cdot 3^2 \cdot 5^4 \cdot 13$.

Proof. We know from Lemma 2.6 that L has a characteristic vector of norm 10. One can fairly easily show that L is unique and that its automorphism group acts transitively on the characteristic vectors of norm 10. The number of characteristic vectors of norm 10 is 624. The stabilizer of V is isomorphic to $\mathrm{Aut}(II_{25,1}, u)$. This is a group of the form $5^3 \cdot 2 \cdot S_5$ (S_5 is the group of all permutations on a set of five elements). [Bor99] □

Now let's relate the Leech lattice to the Conway groups.

3. Relating the Conway groups to the Leech lattice

Now we can get to the cool stuff, after all those definitions! One thing to note is that there is another Conway group Co_0, with order $8,315,553,613,086,720,000$.

Remark 3.1. I did not earlier introduce Co_0 when I was introducing the other Conway groups Co_1, Co_2, and Co_3. This is because Co_0 is not simple, and it should not be thought of as entirely alike the others. However, it still has an interesting property.

Proposition 3.2. *The Conway group* Co_0 *is the group of automorphisms of* Λ_{24} *(addition and inner-product* [6]*).*

Here's an interesting way that the Conway groups Co_0 and Co_1 relate to each other.

Proposition 3.3. *Let* $Z(G)$ *be the center of* Co_0. *We can express* Co_1 *as the quotient of* Co_0 *by* $Z(G)$. [Bor99]

For Co_2 and Co_3, we have the following proposition.

Proposition 3.4. *We have that* Co_2 *and* Co_3 *are isomorphic to subgroups of* Co_1.

The Conway groups are often considered the most important sporadic simple groups. Sadly, John Conway passed away on April 11, 2020. He is well-known for the Game of Life, which he invented. Also, he is remembered for his contributions to finite group theory, combinatorial game theory, coding theory, and numerous other areas of mathematics.

[6] Here, inner-product means the integer value which equals 1/8 the sum of products of the coordinates of two vectors.

4. Constructing Mathieu groups as automorphism groups of Steiner systems

Next we will talk a bit about Mathieu groups, which are another well-known type of sporadic simple group. They are the five smallest sporadic finite simple groups. Let's briefly look at the order of these Mathieu groups: The Mathieu group M_{11} is the sporadic simple group of order

$$2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920.$$

The Mathieu group M_{12} has order

$$2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040$$

(note that this is equal to $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$). The Mathieu group M_{22} has order

$$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443520.$$

The Mathieu group M_{23} has order

$$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 10200960.$$

Finally, M_{24} has order

$$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040.$$

But before we can offer a proper definition/construction of the Mathieu groups, we must first define Steiner systems.

Definition 4.1. For integers $j < k < n$, a collection $S_1, S_2, S_3, \ldots, S_N$ of distinct subsets of $\{1, 2, 3, \ldots, n\}$ is called a (j, k, n)-Steiner system if it satisfies the following:
• For all i, we have $|S_i| = k$.
• For each subset $T \subset \{1, 2, 3, \ldots, n\}$ where $|T| = j$, there is some unique value i such that $S_i \supset T$. [RS11]

Here is the formal construction of the Mathieu groups using Steiner systems:

Definition 4.2. We can define the Mathieu groups using Steiner systems:

$$\bullet M_{11} = \{\sigma \in S_{11} : \sigma(S) \in S(4,5,11) \text{ for all } S \in S(4,5,11)\}$$
$$\bullet M_{12} = \{\sigma \in S_{12} : \sigma(S) \in S(5,6,12) \text{ for all } S \in S(5,6,12)\}$$
$$\bullet M_{22} = \{\sigma \in S_{22} : \sigma(S) \in S(3,6,22) \text{ for all } S \in S(3,6,22)\}$$
$$\bullet M_{23} = \{\sigma \in S_{23} : \sigma(S) \in S(4,7,23) \text{ for all } S \in S(4,7,23)\}$$
$$\bullet M_{24} = \{\sigma \in S_{24} : \sigma(S) \in S(5,8,24) \text{ for all } S \in S(5,8,24)\}.$$

[RS11]

As we can see, the most significant Steiner systems for the construction of Mathieu groups are $S(4, 5, 11)$, $S(5, 6, 12)$, $S(3, 6, 22)$, $S(4, 7, 23)$, and $S(5, 8, 24)$. For more information on Mathieu groups, see Simon Rubinstein-Salzedo's paper, from which I have paraphrased/cited the previous few definitions.

5. The Monster group

At this point, we've looked at the Conway groups and a little bit about Mathieu groups. Another significant group is the Monster group.

Definition 5.1. The *Monster group and Monstrous Moonshine*, which we will denote $\mathbb{M}$, is the largest sporadic simple group; it has order

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$$
$$= 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

This is approximately 8×10^{53}.

Note that there is also a "baby monster" group, which is the second largest (after the Monster/friendly giant) of the sporadic simple groups. One interesting thing about the Monster is that it has 19 of the other sporadic groups as either subquotients or subgroups. Those 19 (or 20, if you count the Monster itself) groups make up the *happy family.* The other 6 are called *pariahs.* Now let's talk about monstrous moonshine, a famous phenomenon whose name was coined by Conway and Norton. First, we will define the j-function (which I have written one of the other papers on).

Definition 5.2. The *j-function* is a function defined on all $\tau \in \mathbb{C}$ (τ can be thought of as an isomorphism class of an elliptic curve), and we have

$$j(\tau) = 12^3 \cdot \frac{g_2(\tau))^3}{g_2(\tau)^3 - 27g_3(\tau)^2},$$

where

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} (m + n\tau)^{-4}$$

and

$$g_3(\tau) = 140 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} (m + n\tau)^{-6}.$$

The *modular discriminant*[7] is defined as

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$$

[7] The modular discriminant is an infinite sum over certain lattice.

in this context. [Sch10]

We refer to the strange relation between the Monster group and the j-function as *monstrous moonshine.* [DMC15] Now let's look at some cool relationships between the j-function and the Monster group, because the j-function is crucial to monstrous moonshine.

Theorem 5.3. *Assume we have an infinite-dimensional graded algebra of the Monster group. The coefficients of the positive powers of q in the q-expansion of $j(\tau)$ are the dimensions of the graded part of the graded algebra.* [Sch10]

Definition 5.4. Abstractly speaking, the *Jabobi identity* tells us how the order of evaluation (layout of parentheses) will work for a given operation.

Definition 5.5. A *Lie algebra* is a collection of vectors (vector space) $\mathfrak{g}$ having a non-associative operation with an alternating bilinear map satisfying the Jacobi identity.

To show an interesting fact about the monster, we first define the following:

Definition 5.6. A *Kac-Moody algebra* is a (infinite-dimensional) Lie algebra which is defined by generators and certain relations (using a generalized Cartan matrix, but that is not so important here). A *generalized Kac-Moody algebra* is also a Lie algebra, and the main difference is that, unlike the regular Kac-Moody algebra, it can have simple imaginary roots.

Now we have an interesting theorem.

Theorem 5.7. *The Monster Lie algebra*[8] *is an infinite-dimensional generalized Kac–Moody algebra. The vector* $(1, -1)$ *gives this algebra one real simple root.*

6. Summary

In this paper, we learnt about the sporadic groups; specifically, we focused on the Conway, Mathieu, and monster groups. In studying these, we saw unimodular lattices (specifically, the Leech lattice and Neimeier lattices) and looked at the proof of a related theorem. Then we related the Conway groups to the Leech lattice. We also saw Steiner systems in our study of Mathieu groups, and we ended by looking at the Monster group (specifically, the Monster Lie algebra).

[8] The *Monster vertex algebra* is loosely defined as an algebra related to the monster group, and it was used to prove the connection between the j-function and the monster group.

References

[Bor99] Richard E Borcherds. The leech lattice and other lattices. *arXiv preprint math/9911195*, 1999.

[CK09] Henry Cohn and Abhinav Kumar. Optimality and uniqueness of the leech lattice among lattices. *Annals of mathematics*, pages 1003–1050, 2009.

[DMC15] John FR Duncan and Sander Mack-Crane. The moonshine module for conway's group. In *Forum of Mathematics, Sigma*, volume 3. Cambridge University Press, 2015.

[RS11] SIMON RUBINSTEIN-SALZEDO. Mathieu groups. 2011.

[Sch10] Asa Scherer. The j-function and the monster. 2010.