Snapshots of modern mathematics
from Oberwolfach

№ 3/2022

Searching for the Monster in the Trees

David A. Craven[1]

The Monster finite simple group is almost unimaginably large, with about 8×10^{53} elements in it. Trying to understand such an immense object requires both theory and computer programs. In this snapshot, we discuss finite groups, representations, and finally Brauer trees, which offer some new understanding of this vast and intricate structure.

Every statistic about the Monster sporadic simple group exudes vastness. It is a mathematical object that consists of the following number of elements:

$$808017424794512875886459904961710757005754368000000000.$$

In the quest to study a set of that size, complex computer programs and algebraic ideas have been harnessed over the past decades, and its structure is slowly becoming clear. The path to this clarity is named "representation theory".

Mathematical objects can be defined purely abstractly. One may define the real numbers as the unique "complete, totally ordered field". Knowing what those words mean doesn't really help you work with the real numbers, but giving a "representation" of them as something more concrete does.

In its broadest sense, a representation of a mathematical object is a way of expressing it in a more approachable fashion. For example, one represents a complex number as a pair (a, b) of real numbers, and then instead of z one writes $a + b\mathrm{i}$ where i stands for a square root of -1. This representation

[1] David A. Craven is supported by the Royal Society.

of complex numbers allows us to add them together incredibly quickly, but multiplication is slightly slower.

Another, different, representation of complex numbers is the polar form which we write as $z = r\mathrm{e}^{\mathrm{i}\theta}$. Here, r is a positive real number which stands for the absolute value of z and θ is a number in $[0, 2\pi)$ which stands for the angle with the positive horizontal axis. Under this representation, multiplication is easy to write down, but now addition becomes more difficult. These two different representations of the complex numbers complement one another; depending on your task, you would choose one or the other (or perhaps an entirely different) representation. For instance, in electronic circuits, you use $a + b\mathrm{i}$,[2] whereas if you are modelling a whirlpool, you would use the polar form.

In algebra, a representation has a stricter definition: it usually involves casting your mathematical concept in terms of matrices. We will get to that later but let's start with a closer look at the concept of groups. The definition of a group was also given in a previous snapshot [6], so read both!

Before looking at it more formally, let me give you the following two examples of groups: the collection of all whole numbers, or *integers*, denoted $\mathbb{Z}$,[3] and the collection of fractions, or *rationals*, denoted $\mathbb{Q}$.[4] For both of these sets of numbers, one may "combine" together any two of those numbers by addition or multiplication and produce a third, and the third always belongs to the set.

A *group* is a set of objects, usually denoted G, with a rule that tells you how to "combine", or "multiply", any two objects in G to produce another one. The multiplication rule[5] must satisfy three properties: The first one is that there is an *identity* object, denoted 1, and for any object x in G, the object $x \cdot 1$—what you obtain when you multiply x and 1 together—is still x, and the same is true of $1 \cdot x$.

Why did I say that both $x \cdot 1$ and $1 \cdot x$ are x? We have *not* required that $x \cdot y$ is always equal to $y \cdot x$. In some groups they are, and in others they are not. If $x \cdot y = y \cdot x$ for any two elements x and y, then the group is called *Abelian*. Both sets $\mathbb{Z}$ and $\mathbb{Q}$ with the usual multiplication rule are Abelian, and $\mathbb{Q}$ is an Abelian group with the usual multiplication, as long as we exclude 0. We will see that this has to do with the impossibility of dividing by 0.[6]

[2] Actually, electrical engineers use j to denote the square root of -1.

[3] It is denoted by $\mathbb{Z}$ because the German word for "integers", *Zahlen*, begins with a "z".

[4] In this case we use $\mathbb{Q}$ because the fancy name for fraction is "quotient".

[5] It has to be emphasized that the group multiplication is rarely the same as the usual multiplication of numbers. For example, we will see later that the set of integers cannot be seen as a group if we use the usual multiplication as the group multiplication rule; however, if we use the usual addition of numbers as the "multiplication" rule, then it works!

[6] Even in the most advanced mathematics, we still don't divide by 0. It's just generally not a good idea, there isn't some kind of super-fantastic math that allows you to do it. Well, sometimes you can, but you have to be *really* careful.

The second property is that, given any object x in G, there is some other object, denoted by x^{-1} and called the *inverse* of x, and this object has the property that $x \cdot x^{-1} = 1$, and so does $x^{-1} \cdot x$. Now we see that $\mathbb{Z}$ is not a group with multiplication rule given by the usual multiplication of numbers, because 2 is in $\mathbb{Z}$, but there is no element 2^{-1} in $\mathbb{Z}$ such that $2 \cdot 2^{-1} = 1$. Such an element is $^1/_2$, which *does* lie in $\mathbb{Q}$, but not in $\mathbb{Z}$. This also explains why 0 needs to be excluded if we want $\mathbb{Q}$ to form a group with the usual multiplication: the element 0 cannot be inverted. On the contrary, the usual addition is a valid "multiplication" rule for both $\mathbb{Z}$ and $\mathbb{Q}$.

The third property is a bit more abstruse: if I give you three objects from $\mathbb{Q}$, called x, y, and z, and ask you to tell me their product, you can do so. But you don't multiply all three together simultaneously, because multiplication is only defined two at a time. So you can multiply x and y together, and then multiply the result by z, or multiply y and z, and then multiply x by $y \cdot z$. We want to get the same answer whichever way you break down the problem. This is called *associativity*. Written in symbols, we have

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

If this holds, it means I don't need to be careful about what I mean by $x \cdot y \cdot z$. There are non-associative structures in mathematics, possibly most importantly "Lie algebras", but most things you can imagine are associative. So the final requirement for G to be a group is that it has the property of associativity.

So we can say now that the Monster group is a huge set with a multiplication rule that has an identity object, all elements have inverses, and the multiplication rule is associative.

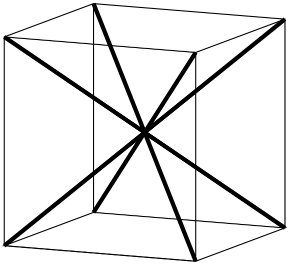
It doesn't look like we have done this, but we have codified in mathematical language the concept of symmetry. The symmetries of anything—a square, Rubik's cube, an equation, a planetary system—form a group. The easiest form of representation in group theory is to be given a group in one form, and then represent it by constructing it as the symmetries of some object.

For instance, consider all ways of moving around four bottles, labelled 1, 2, 3, and 4. We start off with the bottles in order from left to right, 1, 2, 3 and 4, then we swap them in any way. Bottle 1 can be moved to any of the four places, so there are four options for this. Bottle 2 can be put anywhere, except wherever Bottle 1 has gone, so there are three slots it could occupy. Now there are only two places Bottle 3 can fit in, and Bottle 4 is then forced to enter the last open position.

So how many ways are there to move around these four bottles? The first can go to four places, then the second to three places, so there are $12 = 4 \times 3$ different ways to distribute the first two bottles. Then two options for the third means $24 = 4 \times 3 \times 2$ possible ways to move around the first three bottles. Finally, the fourth bottle can only be placed in the last remaining spot, so there are 24 different ways to move around the four bottles.

There are also 24 rotational symmetries of a cube, that is, 24 different ways of how the six faces can be arranged by rotating the cube. To see this, note that a rotation can make any of the six faces be facing down. Once the bottom face has been chosen, we can choose one of the four adjacent faces (but not the face on the top) to be the forward face. Thus there are $24 = 6 \times 4$ possible rotational symmetries of the cube.

Both of these are groups, as one may multiply two rearrangements of $1, 2, 3, 4$ by doing one and then doing the other, and one can multiply rotational symmetries as well, again by doing one, then doing the other. In fact, these two denote "the same" group. The best way to see this is to consider the diagonals of the cube, that is, the lines passing through opposite corners of the cube.



There are four of these, and any rotational symmetry of the cube produces a specific rearrangement of the four diagonals. One can see that in fact this rearrangement of the diagonals determines the rotational symmetry, so we can associate to every rotational symmetry a rearrangement of $1, 2, 3, 4$, and to every rearrangement of $1, 2, 3, 4$ we can associate a rotational symmetry. Furthermore, this function expressing a symmetry of the cube as a rearrangement of four elements satisfies an important property: if you multiply two elements together, and then apply the function, you get the same answer as if you apply the function to the two elements and then multiply them. In notation, we write

$$f(x \cdot y) = f(x) \cdot f(y).$$

A function f between groups with this property is called a *homomorphism.*

Now we can come back to representations. A *representation* of a group is a homomorphism from this given group to a particular group, called the "general linear group". This is the group of "linear transformations" of a space, which is a technical way to say it is the group of all matrices that have an inverse.

Matrices are arrays filled with numbers and there are again rules on how to multiply them, so we can ask whether matrices form a group. This is in general not true: first, if you want to be able to multiply any two matrices that you pick from a set, they all need to have the same number of rows and columns. If the number of rows and columns are the same then you can take the identity matrix I, which is the matrix

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix},$$

and this at least has the property that, for any other matrix M, $M \cdot I = M$ and $I \cdot M = M$. However, if M is a matrix, there is not always a matrix N such that $M \cdot N = I$. This is why we explicitly ask for our matrices to have inverses: for every matrix M we consider, there will be such an inverse matrix N.

So as long as you stick to matrices with inverses, you obtain a group, denoted $\mathrm{GL}_n(\mathbb{F})$, where n is the number of columns (or rows) and where $\mathbb{F}$ is whatever collection of numbers you choose as entries for your matrices (for example, the real numbers or the complex numbers). So a representation is a function from a group G to $\mathrm{GL}_n(\mathbb{F})$ for some n and $\mathbb{F}$.[7]

A rotation in three-dimensional space can be described by a 3 × 3 matrix and it has an inverse (rotating backwards). Therefore, the function from rearrangements of $1, 2, 3, 4$ to rotational symmetries of the cube translates in our new language to a homomorphism from the group S_4 to $\mathrm{GL}_3(\mathbb{R})$. We use the symbol S_4 for the group of all rearrangements of $1, 2, 3, 4$,[8] and $\mathbb{R}$ to denote the real numbers. Similarly, $\mathbb{C}$ denotes the complex numbers.[9]

To start analysing groups, we look at their subgroups. Subgroups are easy to define: a *subgroup* H of a group G is a subset of G that is also a group with the same multiplication. So the non-zero rationals are a subgroup of the non-zero real numbers, with group multiplication being given by the usual multiplication

[7] The letter $\mathbb{F}$ is chosen because it stands for "field". This is like a group, but this time you can add *and* multiply. You can also subtract and divide (but not by zero, see Footnote 6) and it has to satisfy some nice properties, such as associativity for addition and multiplication. The final requirement is that 0 and 1 aren't the same, which you had probably never really worried about before now. The real and complex numbers form fields, but the integers do not, for the same reason they do not form a group with the usual multiplication: you cannot divide.

[8] If we consider all rearrangements of $1, 2, 3, 4, 5$, we write S_5. What do you think S_6 means?

[9] For $\mathbb{R}$ and $\mathbb{C}$, the choice of letters is kind of obvious.

of numbers, because the product of any two rational numbers, that are by definition also real numbers, not only is a real number but even is rational.

We return to our example of S_4, which is called the *symmetric group.* The elements of this group, the rearrangements of $1, 2, 3, 4$, are called *permutations.* There is a beautiful and compact notation for permutations, called *cycle notation.* For example, suppose that bottle 1 moves to where bottle 3 is, pushing bottle 3 out. Bottle 3 has to go somewhere else, so it moves to bottle 4's place, pushing it out. Bottle 4 in turn moves back to the empty space left by bottle 1, and bottle 2 stays where it is. This would be denoted by

$$(1, 3, 4)(2),$$

so the way to read this is that 1 moves to 3, 3 moves to 4, and 4 completes the loop, or cycle, by heading to 1. With this notation, we can easily describe elements of S_4, and indeed S_n for any number n; for example,

$$(1, 6, 3, 9)(2, 7)(4, 10, 8, 11, 12)$$

is a permutation of twelve bottles.[10]

This notation is also very handy to describe the inverse of a permutation. To undo the permutation $(1, 3, 4)$, we have to do $(4, 3, 1)$, so we just read each cycle in the opposite direction.

In order to give a subgroup, we just give one or a few elements of it, and then keep multiplying the elements together until we find every element of the subgroup.[11] The subgroup is then *generated* by the collection with which we started. The subgroup generated by the element $(1, 2, 3, 4)$ consists of the four elements

$$(1, 2, 3, 4), \quad (1, 3)(2, 4), \quad (1, 4, 3, 2), \quad 1.$$

(Check this!) Here 1 stands for the identity element that corresponds to no permutation, that is, $(1)(2)(3)(4)$ in cycle notation. Another example of a subgroup is given by the four elements

$$(1, 2)(3, 4), \quad (1, 3)(2, 4), \quad (1, 4)(2, 3), \quad 1.$$

You can check that if you multiply the first two you obtain the third, and if you multiply the second and third you obtain the first.

The latter subgroup is also "normal". A *normal* subgroup is a subgroup H of G where, if h is an element of H, and g is an element of G, then the product $g^{-1} \cdot h \cdot g$ is always an element of H. If you have studied linear algebra

[10] We often do not write points that are not moved in the permutation, so (5) in this case.

[11] This works if the group is finite. If the group is infinite, we have to include inverses of the chosen elements as well.

before, you might recognize an expression $B^{-1}MB$ as the application of a change of basis matrix B to the matrix M. The idea is similar: a normal subgroup is one that is not moved around by a "change of basis".

Of the two subgroups with four elements above, the first is not normal in S_4 and the second is. To see the first, you can check that

$$(1,2)^{-1} \cdot (1,2,3,4) \cdot (1,2) = (1,3,4,2),$$

which is not in the subgroup.

Normal subgroups of groups are analogous to divisors of an integer: in both cases one may "divide". You know how to divide by a number and there is a construction of a "quotient group", where one divides a group by a subgroup, and we even write G/H to show that we mean a fraction in some sense. This can only work when the subgroup is normal.

If there is an analogue of division for groups, there must be an analogue of being a prime. Indeed, a *simple group* is a group G with no normal subgroups other than G itself and the trivial subgroup just consisting of 1, which is always a normal subgroup, like 1 is always a divisor of any integer. Just as we can write every integer as a product of divisors, we can describe every group through simple groups. For this reason, we are interested in understanding the simple groups.

We focus on *finite* groups now, that is, groups G possessing only a finite number of elements which is denoted by $|G|$. So the symmetric groups S_n are finite groups with $|S_n| = n!$, but the groups $\mathbb{Q}$ and $\mathbb{R}$ (without 0) with multiplication are infinite groups. Combining our notions, we produce the notion of a *finite simple group*, a simple group with only finitely many elements in it.[12] The easiest example of a finite simple group is not the group with one element in it (this is by definition not a simple group, similarly to 1 not being a prime), but the group with two elements in it. The two elements can be denoted by $+1$ and -1, with the usual multiplication. Since there are no subgroups other than itself and 1, it must be simple.

Generalizing the smallest simple group, the *cyclic group* C_n is the subgroup of S_n generated by the single element $(1,2,3,\ldots,n)$. There are exactly n elements in C_n, and every element can be written as a power of the

[12] There are definitely infinite simple groups. And I am definitely not going to talk about them here. There lurk "Tarski[13] monsters", an even more horrible beast than the Monster finite simple group. There's also a Baby Monster. With all these groups being called monsters, I can only assume that group theorists had a lot of nightmares as children.

[13] Yes, the same Tarski as in the Banach–Tarski[14] paradox.

[14] No, an anagram of "Banach Tarski" is not "Banach Tarski Banach Tarski". However, an anagram of "Banach Tarski" is "I ransack Bath". (If you don't understand this joke, check out the Wikipedia entry on the Banach–Tarski paradox.)

element $(1, 2, 3, \ldots, n)$. The group with two elements, ±1, can be also thought of as the group consisting of $(1, 2)$ and 1, hence as the cyclic group C_2. This group C_n turns out to be simple if n is a prime number, so our first family of infinitely many simple groups are the cyclic groups C_p, for p any prime number.

Another type of simple groups is alternating groups. It's fairly easy to believe that one may obtain any permutation of a bunch of objects from repeatedly swapping pairs of objects. Imagine wanting to permute placecards at a dinner table: you make the first swap to place the first person where you want them to go, then another swap to get the second person where they should be, and so on. It turns out that there are lots of different ways to perform a permutation as a sequence of swaps, but these different sequences will either all have an odd number of swaps or all have an even number of swaps in them. So all permutations can be named "even" or "odd" accordingly. An even permutation multiplied by an odd permutation is an odd permutation, and so on, so multiplying permutations looks like adding integers: even times odd is odd, odd times odd is even, and even times even is even. In particular, the even permutations form a subgroup of the symmetric group S_n, called the *alternating group* and denoted by A_n. It can be proven that if n is at least 5 then A_n is always a finite simple group.

There are other finite simple groups though. In fact, we know exactly how many others there are, thanks to a decades-long programme to classify them all, which was finally completed in 1980,[15] in a disparate collection of journal articles published by mathematicians from around the world. The original version, depending on what you consider part of the *Classification of Finite Simple Groups (CFSG)* and what you consider just fun group theory articles, is probably about 8000 pages, although estimates vary. There is a project to write down a coherent and complete proof, which is currently at ten volumes and counting [1, 7]. There's also a project to try to simplify parts of it,[16] in the hope of chopping off a volume or two from the proof.

The result of CFSG is much easier than its proof, although still far beyond what I can say here. Broadly speaking, there are four kinds of simple groups:

1. the cyclic groups C_p for p a prime;
2. the alternating groups A_n for $n \geq 5$;
3. sixteen infinite families of groups of matrices, called *groups of Lie*[17] *type*;
4. twenty-six *sporadic simple groups*, the largest of which is the Monster.

[15] Or 2004, depending on who you talk to.

[16] In fact, two separate projects, but they are happening simultaneously so I'm counting them as one.

[17] Pronounced "lee" rather than "lie". Well, actually it should be pronounced closer to "lee-uh", but people just say "lee" instead.

So here we have our first sight of the Monster. It is one of these sporadic groups, each a single point where happenstance has forced an object into being. If you try to construct a group with certain properties, normally you fail, but in each of these twenty-six cases a unique collection of properties comes together, the circumstances are just right, and a group can be made. There are some patterns in a few of them, and some can be related to one another, but usually when you want to prove something about them, each one must be considered separately.

On the other hand, for groups of Lie type, there is a fiendishly complicated theory, but it is in some sense uniform, so one can often consider all of them at the same time, or at least get some of the way with the problem using general methods before having to switch to a case-by-case analysis.

So now we want to understand these finite simple groups, and one of the most interesting things about them are their representations. Recall that a representation is a homomorphism from a group to some $\mathrm{GL}_n(\mathbb{F})$. Representations have subrepresentations just as groups have subgroups, only this time, like with numbers, given any subrepresentation, one may always quotient out by it, so there's no need to introduce such thing as a "normal" subrepresentation. We therefore have, for a given finite group G, the collection of simple representations of it, that is, the representations that have exactly two subrepresentations. Take one of these simple representations with $\mathbb{F} = \mathbb{C}$, and call it ρ. Then ρ is a function from G to $\mathrm{GL}_n(\mathbb{C})$ for some integer n, and so to every group element we can associate a matrix. To study this further, we look at "traces". The *trace* of a matrix is the sum of the diagonal entries of it:

$$\operatorname{tr}\left(\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}\right) = \sum_{i=1}^{n} a_{ii}.$$

If, for a given representation ρ, one takes the trace of each of the matrices $\rho(g)$ with $g \in G$, one obtains a new function $G \to \mathbb{C}$, called the *character* of the representation ρ.

The theory of characters is beautiful. The characters of all simple representations can be placed in a square table, called the *character table* of a finite group. Each row corresponds to a character and the entries in this row are determined by evaluating that character on a group element. An example of such a table, for the smallest sporadic simple group, the Mathieu group M_{11},

M_{11}	1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	10	2	1	2	0	-1	0	0	-1	-1
χ_3	10	-2	1	0	0	1	$\sqrt{-2}$	$-\sqrt{-2}$	-1	-1
χ_4	10	-2	1	0	0	1	$-\sqrt{-2}$	$\sqrt{-2}$	-1	-1
χ_5	11	3	2	-1	1	0	-1	-1	0	0
χ_6	16	0	-2	0	1	0	0	0	δ	$\bar{\delta}$
χ_7	16	0	-2	0	1	0	0	0	$\bar{\delta}$	δ
χ_8	44	4	-1	0	-1	1	0	0	0	0
χ_9	45	-3	0	1	0	0	-1	-1	1	1
χ_{10}	55	-1	1	-1	0	-1	1	1	0	0

Table 1: The character table of the smallest sporadic group, the Mathieu group M_{11} which has 7920 elements. The element δ is a complex number that is a sum of 11th roots of unity, such that $\delta + \bar{\delta} = -1$ and $|\delta|^2 = 3$.

is given in Table 1.[18] It contains a lot of important numerical data that the expert can use to understand the structure of finite groups.

The character tables of the finite simple groups are reasonably understood: Character tables for cyclic groups are completely understood, and are very easy to write down, for the alternating groups there is a fast formula to find the table, for the groups of Lie type there are general theorems about their shape, but some details still need to be worked out, and as a result of a long collaboration in Cambridge between a group of chain-smoking mathematicians[19], the character tables of all sporadic groups were computed. The character table for the Monster has 194 rows and columns, and even in small print on A3 paper, it takes up eight pages.

But representations are maps from G to $\mathrm{GL}_n(\mathbb{F})$ for a field $\mathbb{F}$, as we said earlier. Character tables capture in its entirety the representation theory for $\mathbb{F} = \mathbb{C}$, but what about other fields? The smallest field has just two elements, 0 and 1, and $1 + 1 = 0$, but all other sums and products behave as you expect. In general, given any prime p, there is a field with that number of elements in it, based on "modular" arithmetic, the same sort of arithmetic you use every time you count the hours in a day. Choose some number n, say $n = 12$. We can

[18] There are really 7920 columns, one for each element, but there are only 10 *different* columns. For example, the second column appears 165 times. If g and h are elements of the group then the columns for h and $g^{-1} \cdot h \cdot g$ are the same, and this is why columns repeat so often.

[19] No, seriously. Apparently the room where these tables were being prepared was full of smoke.

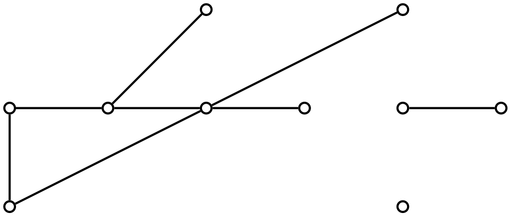


Figure 1: An example of a graph.

define addition and multiplication of integers as usual, but then we divide by n and take remainders. This is how things work in time: if it is 11 o'clock then 15 hours later it will be 2 o'clock, not 26 o'clock.

For $n = 12$, this isn't a field, because a field is supposed to behave like the rationals or reals, and there two non-zero numbers don't multiply together to yield zero, whereas for $n = 12$, we have $2 \times 6 = 0$ (as 0 is the remainder upon division by 12). One can only make a field if n is a prime, but if this is the case, then this process constructs a field, where you can add, subtract, multiply, and divide[20] to your heart's content. This field is denoted by $\mathbb{F}_p$.

Representation theory over $\mathbb{F}_p$ can be studied whenever the prime p divides the number of elements $|G|$. However, it is much more difficult than over $\mathbb{C}$, and we are still far away from understanding what is going on. One case, that is still within our grasp, though, is where p divides $|G|$ but p^2 does not divide $|G|$. For instance, if $G = S_5$, then $|G| = 120$, and 120 factorizes as $2^3 \cdot 3 \cdot 5$, so the possibilities for such a p are 3 and 5 for this group.

Here one may describe the relationship between the representation theories over $\mathbb{C}$ and $\mathbb{F}_p$ using a picture, called a "Brauer tree" which is a specific graph. A *graph* is a collection of points—called *vertices*—with lines—called *edges*—connecting some pairs of vertices. As an example, see Figure 1. A *tree* is a graph where you can travel along edges to get from any vertex to any other in exactly one way. To any group G and any prime p where p divides $|G|$ but p^2 does not, one may associate a collection of trees, called *Brauer trees*, that allows us to describe with some pictures the representation theory of G over both $\mathbb{C}$ and $\mathbb{F}_p$ simultaneously. This is a fantastic achievement, one that has not been replicated for any prime p where p^2 divides $|G|$.[21]

[20] Except by zero...

[21] This remains one of the most ambitious goals of group representation theory, to be able to get as much a grasp on the general case as we have on the special case with Brauer trees.

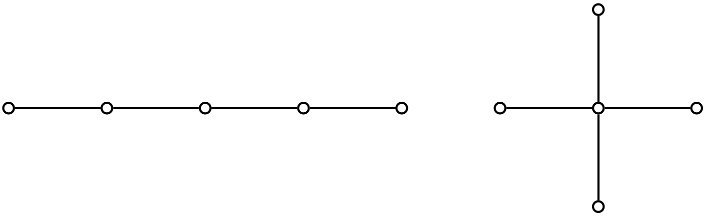


Figure 2: A line (left) and a star (right).

The vertices of this graph are labelled by the characters of G that come from the character table, and the edges by the simple representations over $\mathbb{F}_p$. Knowing which two characters are connected by an edge gives us enough data to construct every representation of G over $\mathbb{F}_p$, not just the simple ones.

It turns out that most Brauer trees are either lines or stars, as in Figure 2. An article by Walter Feit in the 1980s [4] shows that we can obtain all Brauer trees of finite groups just by looking at the Brauer trees of finite simple groups.[22] So we need to look through the list of finite simple groups, finding all their Brauer trees.

Brauer trees of cyclic groups are just a single edge between two vertices, so are easy to describe. Those of symmetric and alternating groups were found decades ago. They appear in the work of Gilbert de Beauregard Robinson in the early 1960s [8], and they all are either lines, or a cross between a line and a star, called a "windmill", which looks like blades of a windmill. For groups of Lie type, many Brauer trees are lines again, although some can be more funky. Paul Fong and Bhama Srinivasan [5] (see also Feit [4]) determined them for six families of groups of Lie type, called "classical" groups. For the other ten families, of "exceptional" groups, many trees had been found over the decades. Finally, the most difficult trees were solved in a work of Olivier Dudas, Raphaël Rouquier, and myself [2], and a work of Radha Kessar and myself [3][23], so the trees for groups of Lie type are (with one exception) completely known.

Thus all Brauer trees are known for the cyclic groups, alternating groups, and more or less for the groups of Lie type. What about the sporadic simple

[22] Technically, he proved that you need only consider "quasisimple" groups, which are very close, but not exactly the same as simple groups.

[23] This last work determines the trees of what are known as "isolated blocks", but there is a single tree that we have not completely determined at the time of writing, and there are two possibilities for it. The theoretical methods we have give constraints on the possible shapes of the trees: the number of vertices, the total number of edges coming out of each vertex, and so on. The constraints are enough to determine the tree uniquely, except for this one outstanding, and very frustrating, case. All other trees are now known, though.

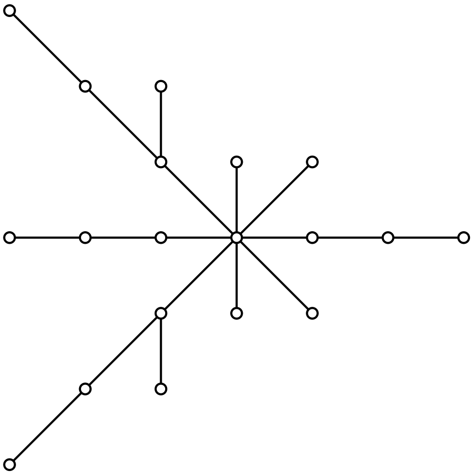


Figure 3: A Brauer tree for the Thompson sporadic simple group.

groups? Some of the techniques used in previous cases work here as well, but not others. Everything ends up being shoved into a big computer, and we hope that the information we can glean is enough to determine the trees uniquely. For example, Figure 3 gives a Brauer tree for the Thompson sporadic group and $p = 19$.

In fact, we can determine all trees with this method, *except* for two of the groups: the Baby Monster and the Monster. For each of them, some of the trees can be constructed, but not all of the edges can be placed on the trees. The number of elements in the Monster was given at the start of this article, and factorized this number is

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

The Brauer trees are known for $p = 17, 19, 23, 31$, but are still out of reach for $p = 29, 41, 47, 59, 71$. We need a new idea[24] to obtain these final trees and unlock more of the Monster's secrets.

[24] There's been a couple of new ideas recently, but unfortunately the new idea also needs to work.

References

[1] M. Aschbacher and S. D. Smith, *The classification of quasithin groups (2 vols)*, vol. 111–112, American Mathematical Society, 2004.

[2] D. A. Craven, O. Dudas, and R. Rouquier, *Brauer trees of unipotent blocks*, Journal of the European Mathematical Society **22** (2020), 2821–2877.

[3] D. A. Craven and R. Kessar, *Brauer trees of isolated blocks of finite groups of Lie type*, in preparation.

[4] W. Feit, *Possible Brauer trees*, Illinois Journal of Mathematics **28** (1984), 43–56.

[5] P. Fong and B. Srinivasan, *Brauer trees in classical groups*, Journal of Algebra **131** (1990), no. 1, 179–225.

[6] E. Giannelli and J. Taylor, *Symmetry and characters of finite groups*, Snapshots of modern mathematics from Oberwolfach (2016), no. 05, http://publications.mfo.de/handle/mfo/460.

[7] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups (8 vols)*, vol. 40, American Mathematical Society, 1996–2018.

[8] G. de B. Robinson, *Representation theory of the symmetric group*, Mathematical expositions. University of Toronto Press, VIII, 1961.

David A. Craven *is a Senior Birmingham Fellow in pure mathematics at the University of Birmingham.*

Mathematical subjects
Algebra and Number Theory

License
Creative Commons BY-SA 4.0

DOI
10.14760/SNAP-2022-003-EN

Snapshots of modern mathematics from Oberwolfach provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

ISSN 2626-1995

Junior Editors
Anja Randecker, Jan Kohlrus
junior-editors@mfo.de

Senior Editor
Anja Randecker
senior-editor@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9 – 11
77709 Oberwolfach
Germany

Director
Gerhard Huisken

Mathematisches
Forschungsinstitut
Oberwolfach

Member of Leibniz
Leibniz Association

IMAGINARY
open mathematics