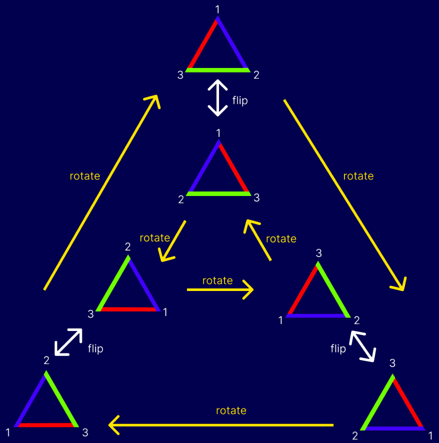
Finite Group Theory: the major problems, and why we care



The formal definition of a group is one we've all seen many times:

Definition

A *group* is a pair $(G, \circ)$ where G is a set, and $\circ : G \times G \to G$ is a binary operation on G that satisfies the following three properties:

(i) **Associativity**. For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$.

(ii) **Identity**. G has an element, which we call 1_G, satisfying $g \circ 1_G = 1_G \circ g = g$ for all $g \in G$. We call 1_G an *identity element* in $(G, \circ)$.

(iii) **Inverse**. For all $g \in G$, there exists an element in G, which we call g^{-1}, satisfying $g \circ g^{-1} = g^{-1} \circ g = 1_G$, where 1_G is as in (ii). We call g^{-1} an *inverse* of g in $(G, \circ)$.

The formal definition of a group is one we've all seen many times:

Definition

A *group* is a pair $(G, \circ)$ where G is a set, and $\circ : G \times G \to G$ is a binary operation on G that satisfies the following three properties:

(i) **Associativity**. For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$.

(ii) **Identity**. G has an element, which we call 1_G, satisfying $g \circ 1_G = 1_G \circ g = g$ for all $g \in G$. We call 1_G an *identity element* in $(G, \circ)$.

(iii) **Inverse**. For all $g \in G$, there exists an element in G, which we call g^{-1}, satisfying $g \circ g^{-1} = g^{-1} \circ g = 1_G$, where 1_G is as in (ii). We call g^{-1} an *inverse* of g in $(G, \circ)$.

But what is the point of this? Is it abstract nonsense, or is there a purpose (beyond the fun of it)?

The formal definition of a group is one we've all seen many times:

Definition

A *group* is a pair $(G, \circ)$ where G is a set, and $\circ : G \times G \to G$ is a binary operation on G that satisfies the following three properties:

(i) **Associativity**. For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$.

(ii) **Identity**. G has an element, which we call 1_G, satisfying $g \circ 1_G = 1_G \circ g = g$ for all $g \in G$. We call 1_G an *identity element* in $(G, \circ)$.

(iii) **Inverse**. For all $g \in G$, there exists an element in G, which we call g^{-1}, satisfying $g \circ g^{-1} = g^{-1} \circ g = 1_G$, where 1_G is as in (ii). We call g^{-1} an *inverse* of g in $(G, \circ)$.

But what is the point of this? Is it abstract nonsense, or is there a purpose (beyond the fun of it)?

Most branches of algebra we study today (i.e. Linear Algebra; Ring Theory; Group Theory; Module Theory, etc.) were built from a desire to get rigorous answers to questions from other areas of mathematics and science.

For example, building on ideas from both ancient China and ancient Greece, Linear Algebra emerged in Europe in the 16th century as a method to rigorously study various problems in Geometry, such as intersections of planes, lines and other geometric objects.

For example, building on ideas from both ancient China and ancient Greece, Linear Algebra emerged in Europe in the 16th century as a method to rigorously study various problems in Geometry, such as intersections of planes, lines and other geometric objects.

Group Theory, on the other hand, discovered by Galois in the 19th century, is the mechanism by which mathematicians understand symmetry.

For example, building on ideas from both ancient China and ancient Greece, Linear Algebra emerged in Europe in the 16th century as a method to rigorously study various problems in Geometry, such as intersections of planes, lines and other geometric objects.

Group Theory, on the other hand, discovered by Galois in the 19th century, is the mechanism by which mathematicians understand symmetry.

While numbers are abstract mathematical objects that allow us to represent counting, *Groups* are abstract mathematical objects that allow us to represent symmetry.

For example, building on ideas from both ancient China and ancient Greece, Linear Algebra emerged in Europe in the 16th century as a method to rigorously study various problems in Geometry, such as intersections of planes, lines and other geometric objects.

Group Theory, on the other hand, discovered by Galois in the 19th century, is the mechanism by which mathematicians understand symmetry.

While numbers are abstract mathematical objects that allow us to represent counting, *Groups* are abstract mathematical objects that allow us to represent symmetry.

As with the branches of algebra of mentioned above, the definition of the *objects* in Group Theory (i.e. groups) is entirely motivated by their scientific purpose: the desire to understand symmetry..

For example, building on ideas from both ancient China and ancient Greece, Linear Algebra emerged in Europe in the 16th century as a method to rigorously study various problems in Geometry, such as intersections of planes, lines and other geometric objects.

Group Theory, on the other hand, discovered by Galois in the 19th century, is the mechanism by which mathematicians understand symmetry.

While numbers are abstract mathematical objects that allow us to represent counting, *Groups* are abstract mathematical objects that allow us to represent symmetry.

As with the branches of algebra of mentioned above, the definition of the *objects* in Group Theory (i.e. groups) is entirely motivated by their scientific purpose: the desire to understand symmetry..

Let's look back at the definition:

Definition

A *group* is a pair $(G, \circ)$ where G is a set, and $\circ : G \times G \to G$ is a binary operation on G that satisfies the following three properties:

(i) **Associativity**. For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$.

(ii) **Identity**. G has an element, which we call 1_G, satisfying $g \circ 1_G = 1_G \circ g = g$ for all $g \in G$. We call 1_G an *identity element* in $(G, \circ)$.

(iii) **Inverse**. For all $g \in G$, there exists an element in G, which we call g^{-1}, satisfying $g \circ g^{-1} = g^{-1} \circ g = 1_G$, where 1_G is as in (ii). We call g^{-1} an *inverse* of g in $(G, \circ)$.

Part (i) represents the fact that, if I perform two symmetries (g and h) and then perform another (k) some time later; this is the same as performing g, waiting a while, then performing h and k.

Definition

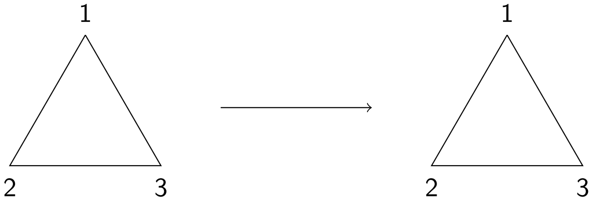
A *group* is a pair $(G, \circ)$ where G is a set, and $\circ : G \times G \to G$ is a binary operation on G that satisfies the following three properties:

(i) **Associativity**. For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$.

(ii) **Identity**. G has an element, which we call 1_G, satisfying $g \circ 1_G = 1_G \circ g = g$ for all $g \in G$. We call 1_G an *identity element* in $(G, \circ)$.

(iii) **Inverse**. For all $g \in G$, there exists an element in G, which we call g^{-1}, satisfying $g \circ g^{-1} = g^{-1} \circ g = 1_G$, where 1_G is as in (ii). We call g^{-1} an *inverse* of g in $(G, \circ)$.

In part (ii), the identity represents the "do nothing" symmetry of an object.



Definition

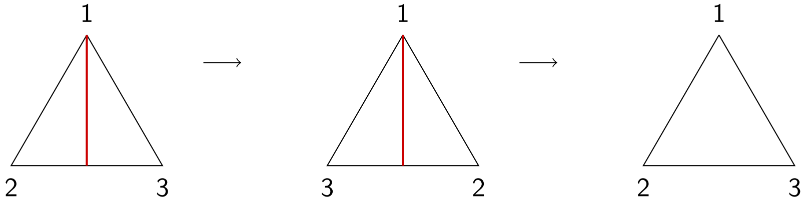
A *group* is a pair $(G, \circ)$ where G is a set, and $\circ : G \times G \to G$ is a binary operation on G that satisfies the following three properties:

(i) **Associativity**. For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$.

(ii) **Identity**. G has an element, which we call 1_G, satisfying $g \circ 1_G = 1_G \circ g = g$ for all $g \in G$. We call 1_G an *identity element* in $(G, \circ)$.

(iii) **Inverse**. For all $g \in G$, there exists an element in G, which we call g^{-1}, satisfying $g \circ g^{-1} = g^{-1} \circ g = 1_G$, where 1_G is as in (ii). We call g^{-1} an *inverse* of g in $(G, \circ)$.

Part (iii) encodes the fact the "reverse" of every symmetry is still a symmetry.



We've just looked at the symmetries of an equilateral triangle (i.e. a regular 3-gon). There are $2n$ symmetries of a regular n-gon (made up of n reflections and n rotations), and the group they constitute is called the dihedral group D_{2n}.

We've just looked at the symmetries of an equilateral triangle (i.e. a regular 3-gon). There are $2n$ symmetries of a regular n-gon (made up of n reflections and n rotations), and the group they constitute is called the dihedral group D_{2n}.

More generally, the group of symmetries of an n element set (or equivalently the number of shuffles of a pack of n cards) is called the symmetric group of degree n, and is written S_n.

We've just looked at the symmetries of an equilateral triangle (i.e. a regular 3-gon). There are $2n$ symmetries of a regular n-gon (made up of n reflections and n rotations), and the group they constitute is called the dihedral group D_{2n}.

More generally, the group of symmetries of an n element set (or equivalently the number of shuffles of a pack of n cards) is called the symmetric group of degree n, and is written S_n.

There are many more symmetries of an n elements set (indeed, $|S_n| = n!$) than a regular n-gon, since symmetries there are much less restrictive.

We've just looked at the symmetries of an equilateral triangle (i.e. a regular 3-gon). There are $2n$ symmetries of a regular n-gon (made up of n reflections and n rotations), and the group they constitute is called the dihedral group D_{2n}.

More generally, the group of symmetries of an n element set (or equivalently the number of shuffles of a pack of n cards) is called the symmetric group of degree n, and is written S_n.

There are many more symmetries of an n elements set (indeed, $|S_n| = n!$) than a regular n-gon, since symmetries there are much less restrictive.

Historical note: The first definition of a group was given by Galois in 1830, and it was less abstract than the one above. Indeed, Galois defined *a group of substitutions of degree n* to be what we now call a subgroup of the symmetric group S_n. This shows that the study of groups is fundamentally motivated by the desire to understand symmetry.

Galois' definition shows that the study of groups is fundamentally motivated by the desire to understand symmetry.

Because symmetry is so universal, Group Theory is highly ubiquitous: it arises naturally not only in many fundamental areas of mathematics (like Geometry, Topology, Number Theory, Harmonic Analysis and more); but also in other areas of human study (like Virology, Chemistry, Physics, Computer Science, Cryptography..).

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

E.g. For a prime p, there is only one finite group of order p: the cyclic group C_p (also called $\mathbb{Z}/p\mathbb{Z}$).

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

E.g. For a prime p, there is only one finite group of order p: the cyclic group C_p (also called $\mathbb{Z}/p\mathbb{Z}$).

E.g. There are two finite groups of order 6, namely the cyclic group C_6 and the symmetric group S_3 of degree 3.

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

E.g. For a prime p, there is only one finite group of order p: the cyclic group C_p (also called $\mathbb{Z}/p\mathbb{Z}$).

E.g. There are two finite groups of order 6, namely the cyclic group C_6 and the symmetric group S_3 of degree 3.

E.g. There are five finite groups of order 8, namely C_8; $C_4 \times C_2$; $C_2 \times C_2 \times C_2$; the dihedral group D_8; and the quaternion group Q_8.

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

E.g. For a prime p, there is only one finite group of order p: the cyclic group C_p (also called $\mathbb{Z}/p\mathbb{Z}$).

E.g. There are two finite groups of order 6, namely the cyclic group C_6 and the symmetric group S_3 of degree 3.

E.g. There are five finite groups of order 8, namely C_8; $C_4 \times C_2$; $C_2 \times C_2 \times C_2$; the dihedral group D_8; and the quaternion group Q_8.

If you've done MA3K4, you will also have seen the classification of groups of order $4p$ and $2p^2$ (for p prime), for example.

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

E.g. For a prime p, there is only one finite group of order p: the cyclic group C_p (also called $\mathbb{Z}/p\mathbb{Z}$).

E.g. There are two finite groups of order 6, namely the cyclic group C_6 and the symmetric group S_3 of degree 3.

E.g. There are five finite groups of order 8, namely C_8; $C_4 \times C_2$; $C_2 \times C_2 \times C_2$; the dihedral group D_8; and the quaternion group Q_8.

If you've done MA3K4, you will also have seen the classification of groups of order $4p$ and $2p^2$ (for p prime), for example.

The most major of the major problems in finite group theory is closely related to this, and is called the *Extension Problem*.

Finite group theory: What are the major problems?

In early courses in group theory, one usually sees how to classify groups of small order.

E.g. For a prime p, there is only one finite group of order p: the cyclic group C_p (also called $\mathbb{Z}/p\mathbb{Z}$).

E.g. There are two finite groups of order 6, namely the cyclic group C_6 and the symmetric group S_3 of degree 3.

E.g. There are five finite groups of order 8, namely C_8; $C_4 \times C_2$; $C_2 \times C_2 \times C_2$; the dihedral group D_8; and the quaternion group Q_8.

If you've done MA3K4, you will also have seen the classification of groups of order $4p$ and $2p^2$ (for p prime), for example.

The most major of the major problems in finite group theory is closely related to this, and is called the *Extension Problem*.

The Extension Problem

Classify all of the finite groups.

For various other values of n (always with hard restrictions on the prime divisors of n), the finite groups of order n have been classified.

In particular, we know the finite groups of order up as far as $2047 = 2^{11} - 1$. Here are the number of groups of order 2^k, for $k \leq 10$.

For various other values of n (always with hard restrictions on the prime divisors of n), the finite groups of order n have been classified.

In particular, we know the finite groups of order up as far as $2047 = 2^{11} - 1$. Here are the number of groups of order 2^k, for $k \leq 10$.

$\lvert G \rvert$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

For various other values of n (always with hard restrictions on the prime divisors of n), the finite groups of order n have been classified.

In particular, we know the finite groups of order up as far as $2047 = 2^{11} - 1$. Here are the number of groups of order 2^k, for $k \leq 10$.

$\lvert G \rvert$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2.

For various other values of n (always with hard restrictions on the prime divisors of n), the finite groups of order n have been classified.

In particular, we know the finite groups of order up as far as $2047 = 2^{11} - 1$. Here are the number of groups of order 2^k, for $k \leq 10$.

$\lvert G \rvert$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2.

In fact, around 99.1% have order 2^{10}.

For various other values of n (always with hard restrictions on the prime divisors of n), the finite groups of order n have been classified.

In particular, we know the finite groups of order up as far as $2047 = 2^{11} - 1$. Here are the number of groups of order 2^k, for $k \leq 10$.

$\lvert G \rvert$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2.

In fact, around 99.1% have order 2^{10}.

We will come back to this heuristic later in the talk, but for now...

Moral of the story: In general, the Extension Problem is intractable! For this reason, group theorists focus on other questions/areas, which aim to get us as close to a solution to the Extension Problem as possible. For the remainder of the talk, I will speak about three of these questions/areas:

1. The Classification of Finite Simple Groups;
2. Asymptotic group theory;
3. Burnside's problems.

1. The Classification of Finite Simple Groups

Back to the extension problem

Recall from above, the ultimate goal of finite group theorists:

The Extension Problem

Classify all of the finite groups.

Back to the extension problem

Recall from above, the ultimate goal of finite group theorists:

The Extension Problem

Classify all of the finite groups.

As mentioned, the Extension Problem, in full generality, is intractable (at least at the moment..).

But as we saw before, we can classify some classes of finite groups (e.g. those of prime order; those of order p^2 or $2p^2$ for a prime p, and much more.)

Back to the extension problem

Recall from above, the ultimate goal of finite group theorists:

The Extension Problem

Classify all of the finite groups.

As mentioned, the Extension Problem, in full generality, is intractable (at least at the moment..).

But as we saw before, we can classify some classes of finite groups (e.g. those of prime order; those of order p^2 or $2p^2$ for a prime p, and much more.)

One particularly important class of finite groups are the *finite simple groups*, i.e. the finite groups G in which the only normal subgroups are $\{1_G\}$ and G itself.

Back to the extension problem

Recall from above, the ultimate goal of finite group theorists:

The Extension Problem

Classify all of the finite groups.

As mentioned, the Extension Problem, in full generality, is intractable (at least at the moment..).

But as we saw before, we can classify some classes of finite groups (e.g. those of prime order; those of order p^2 or $2p^2$ for a prime p, and much more.)

One particularly important class of finite groups are the *finite simple groups*, i.e. the finite groups G in which the only normal subgroups are $\{1_G\}$ and G itself.

But why are the finite simple groups so important?

The Jordan–Hölder theorem

Theorem (Jordan–Hölder theorem)

Every finite group G has a composition series, i.e. a series

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$$

such that for each $1 \leq i \leq r$, the group G_i/G_{i-1} is simple. Moreover, although there can be different composition series, the length r, and the isomorphism classes of the factors G_i/G_{i-1} do not change. Thus, the multiset $\{\{G_i/G_{i-1} : 1 \leq i \leq r\}\}$ is well-defined, and is called the set of composition factors for G.

The Jordan–Hölder theorem

Theorem (Jordan–Hölder theorem)

Every finite group G has a composition series, i.e. a series

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$$

such that for each $1 \leq i \leq r$, the group G_i/G_{i-1} is simple. Moreover, although there can be different composition series, the length r, and the isomorphism classes of the factors G_i/G_{i-1} do not change. Thus, the multiset $\{\{G_i/G_{i-1} : 1 \leq i \leq r\}\}$ is well-defined, and is called the set of composition factors for G.

E.g. The alternating groups A_n are simple for $n \geq 5$, while the cyclic groups of prime order are simple. The composition factors of S_n for $n \geq 5$ are $\{\{A_n, C_2\}\}$.

E.g. For p an odd prime, the composition factors of the dihedral group D_{2p} of order $2p$ are $\{\{C_p, C_2\}\}$.

This is why group theorists often refer to the finite simple groups as the *building blocks of the finite groups*. In a certain sense, they are thought of as analogous to the primes in number theory.

This is why group theorists often refer to the finite simple groups as the *building blocks of the finite groups*. In a certain sense, they are thought of as analogous to the primes in number theory.

For this reason, understanding the finite simple groups is crucial if one wants to get anywhere near the Extension Problem..

This is why group theorists often refer to the finite simple groups as the *building blocks of the finite groups*. In a certain sense, they are thought of as analogous to the primes in number theory.

For this reason, understanding the finite simple groups is crucial if one wants to get anywhere near the Extension Problem..

In the courses MA3K4: *Introduction to Group Theory* and MA442: *Group Theory* at Warwick, one sees some of the early ideas group theorists used to increase our understanding of the finite simple groups.

This is why group theorists often refer to the finite simple groups as the *building blocks of the finite groups*. In a certain sense, they are thought of as analogous to the primes in number theory.

For this reason, understanding the finite simple groups is crucial if one wants to get anywhere near the Extension Problem..

In the courses MA3K4: *Introduction to Group Theory* and MA442: *Group Theory* at Warwick, one sees some of the early ideas group theorists used to increase our understanding of the finite simple groups.

For example, in Chapter 3 of MA3K4, we use Sylow's theorems to show that various groups (for example groups of order $4p^n$) cannot be simple, while in MA442, Sylow's theorems (and various other ideas, such as Burnside's transfer theorem) are used to classify the finite simple groups of order at most 500).

This is why group theorists often refer to the finite simple groups as the *building blocks of the finite groups*. In a certain sense, they are thought of as analogous to the primes in number theory.

For this reason, understanding the finite simple groups is crucial if one wants to get anywhere near the Extension Problem..

In the courses MA3K4: *Introduction to Group Theory* and MA442: *Group Theory* at Warwick, one sees some of the early ideas group theorists used to increase our understanding of the finite simple groups.

For example, in Chapter 3 of MA3K4, we use Sylow's theorems to show that various groups (for example groups of order $4p^n$) cannot be simple, while in MA442, Sylow's theorems (and various other ideas, such as Burnside's transfer theorem) are used to classify the finite simple groups of order at most 500).

The most famous early theorem in this direction used deep applications of these ideas to prove the following:

This is why group theorists often refer to the finite simple groups as the *building blocks of the finite groups*. In a certain sense, they are thought of as analogous to the primes in number theory.

For this reason, understanding the finite simple groups is crucial if one wants to get anywhere near the Extension Problem..

In the courses MA3K4: *Introduction to Group Theory* and MA442: *Group Theory* at Warwick, one sees some of the early ideas group theorists used to increase our understanding of the finite simple groups.

For example, in Chapter 3 of MA3K4, we use Sylow's theorems to show that various groups (for example groups of order $4p^n$) cannot be simple, while in MA442, Sylow's theorems (and various other ideas, such as Burnside's transfer theorem) are used to classify the finite simple groups of order at most 500).

The most famous early theorem in this direction used deep applications of these ideas to prove the following:

Theorem (Burnside's $p^a q^b$ theorem)

Let p and q be primes, and let G be a group of order $p^a q^b$. Then G is not simple.

Then in the 1970s, there was an even more breathtaking advancement in our understanding of the finite simple groups.

Theorem (The Odd Order Theorem; Feit & Thompson, 1970)

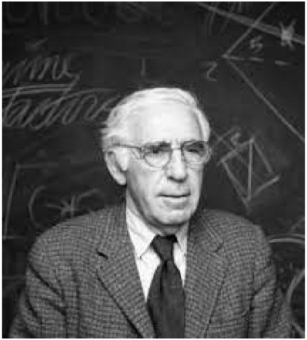
Let G be a finite group of odd order. Then G is not simple.

Then in the 1970s, there was an even more breathtaking advancement in our understanding of the finite simple groups.

Theorem (The Odd Order Theorem; Feit & Thompson, 1970)

Let G be a finite group of odd order. Then G is not simple.

Encouraged by this, together with some other deep results on finite simple groups like the Brauer-Fowler theorem, Daniel Gorenstein announced in 1972 an ambitious 16 step programme that would classify the finite simple groups.



The Classification of Finite Simple Groups

In a nutshell, the idea of the proof proceeds by first listing the known finite simple groups:

- the cyclic groups C_p of prime order p;

The Classification of Finite Simple Groups

In a nutshell, the idea of the proof proceeds by first listing the known finite simple groups:

- the cyclic groups C_p of prime order p;
- the alternating groups A_n of degree $n \geq 5$;

The Classification of Finite Simple Groups

In a nutshell, the idea of the proof proceeds by first listing the known finite simple groups:

- the cyclic groups C_p of prime order p;
- the alternating groups A_n of degree $n \geq 5$;
- the finite groups of Lie type (these are essentially matrix groups, e.g. $\mathbf{PSL}_n(\mathbb{F})$ for $n \geq 1$, $\mathbb{F}$ a finite field, and $(n, |\mathbb{F}|) \notin \{(2,2),(2,3)\}$); and

The Classification of Finite Simple Groups

In a nutshell, the idea of the proof proceeds by first listing the known finite simple groups:

- the cyclic groups C_p of prime order p;
- the alternating groups A_n of degree $n \geq 5$;
- the finite groups of Lie type (these are essentially matrix groups, e.g. $\mathbf{PSL}_n(\mathbb{F})$ for $n \geq 1$, $\mathbb{F}$ a finite field, and $(n, |\mathbb{F}|) \notin \{(2,2),(2,3)\}$); and
- the 26 sporadic simple groups.

The Classification of Finite Simple Groups

In a nutshell, the idea of the proof proceeds by first listing the known finite simple groups:

- the cyclic groups C_p of prime order p;
- the alternating groups A_n of degree $n \geq 5$;
- the finite groups of Lie type (these are essentially matrix groups, e.g. $\mathbf{PSL}_n(\mathbb{F})$ for $n \geq 1$, $\mathbb{F}$ a finite field, and $(n, |\mathbb{F}|) \notin \{(2,2),(2,3)\}$); and
- the 26 sporadic simple groups.

Side note: The last category is a set of finite simple groups of order between 7920 (the order of the *Mathieu group* M_{11}) and

$$808017424794512875886459904961710757005754368000000000 \sim 10^{53}$$

(the order of the *monster group* M).

The Classification of Finite Simple Groups

In a nutshell, the idea of the proof proceeds by first listing the known finite simple groups:

- the cyclic groups C_p of prime order p;
- the alternating groups A_n of degree $n \geq 5$;
- the finite groups of Lie type (these are essentially matrix groups, e.g. $\mathbf{PSL}_n(\mathbb{F})$ for $n \geq 1$, $\mathbb{F}$ a finite field, and $(n, |\mathbb{F}|) \notin \{(2,2),(2,3)\}$); and
- the 26 sporadic simple groups.

Side note: The last category is a set of finite simple groups of order between 7920 (the order of the *Mathieu group* M_{11}) and

$$808017424794512875886459904961710757005754368000000000 \sim 10^{53}$$

(the order of the *monster group* M).

These groups do not fit naturally into any of the preceding three infinite families.

Gorenstein's programme

In pursuit of a contradiction, one then chooses a finite simple group G such that G is not one of those listed above, and $|G|$ is as small as possible.

Gorenstein's programme

In pursuit of a contradiction, one then chooses a finite simple group G such that G is not one of those listed above, and $|G|$ is as small as possible.

From the previous theorems, we know that G has even order, and that $|G|$ has at least 3 prime divisors. The Brauer-Fowler theorem also gives us information about the centralisers of elements of order 2 in G; while a method due to Bender gives certain restrictions on the maximal subgroups of G.

Gorenstein's programme

In pursuit of a contradiction, one then chooses a finite simple group G such that G is not one of those listed above, and $|G|$ is as small as possible.

From the previous theorems, we know that G has even order, and that $|G|$ has at least 3 prime divisors. The Brauer-Fowler theorem also gives us information about the centralisers of elements of order 2 in G; while a method due to Bender gives certain restrictions on the maximal subgroups of G.

The minimality of $|G|$ also shows that all subgroups of G have their composition factors lying in our know list of finite simple groups..

The successful completion of this programme, and hence the Classification of Finite Simple Groups was announced by Gorenstein in 1983.

The successful completion of this programme, and hence the Classification of Finite Simple Groups was announced by Gorenstein in 1983.

Despite Gorenstein's announcement, there was a gap in the proof, which wasn't completed until 2004, and took an extra 1000 pages to sort out (done by M. Aschbacher and S. Smith).

The successful completion of this programme, and hence the Classification of Finite Simple Groups was announced by Gorenstein in 1983.

Despite Gorenstein's announcement, there was a gap in the proof, which wasn't completed until 2004, and took an extra 1000 pages to sort out (done by M. Aschbacher and S. Smith).

In total, the theorem comprises work by around 100 different authors, and the proof, in its entirety, is about 10000 pages in length.

The successful completion of this programme, and hence the Classification of Finite Simple Groups was announced by Gorenstein in 1983.

Despite Gorenstein's announcement, there was a gap in the proof, which wasn't completed until 2004, and took an extra 1000 pages to sort out (done by M. Aschbacher and S. Smith).

In total, the theorem comprises work by around 100 different authors, and the proof, in its entirety, is about 10000 pages in length.

It is one of the most significant achievements of 20th century mathematics, though the New York Times were a little more downbeat, with the headline:

The successful completion of this programme, and hence the Classification of Finite Simple Groups was announced by Gorenstein in 1983.

Despite Gorenstein's announcement, there was a gap in the proof, which wasn't completed until 2004, and took an extra 1000 pages to sort out (done by M. Aschbacher and S. Smith).

In total, the theorem comprises work by around 100 different authors, and the proof, in its entirety, is about 10000 pages in length.

It is one of the most significant achievements of 20th century mathematics, though the New York Times were a little more downbeat, with the headline:

"Mathematicians theorize themselves out of a job"

the day after the announcement, in 1983.

Why are the New York Times wrong?

There is no doubt that the CFSG has been a monumental advancement in our goal to understand the finite groups. But we are still nowhere near a complete understanding (as we have of vector spaces in linear algebra, for example).

Why are the New York Times wrong?

There is no doubt that the CFSG has been a monumental advancement in our goal to understand the finite groups. But we are still nowhere near a complete understanding (as we have of vector spaces in linear algebra, for example).

There are a few reasons for this.

Why are the New York Times wrong?

There is no doubt that the CFSG has been a monumental advancement in our goal to understand the finite groups. But we are still nowhere near a complete understanding (as we have of vector spaces in linear algebra, for example).

There are a few reasons for this.

Although we now know what the building blocks of the finite groups are, we have no idea how to "glue" them together! That is, given a multisets C of finite simple groups, we have no idea how many, or what kind of, finite groups have C as their set of composition factors. So we are still very far away from solving the extension problem..

Why are the New York Times wrong?

There is no doubt that the CFSG has been a monumental advancement in our goal to understand the finite groups. But we are still nowhere near a complete understanding (as we have of vector spaces in linear algebra, for example).

There are a few reasons for this.

Although we now know what the building blocks of the finite groups are, we have no idea how to "glue" them together! That is, given a multisets C of finite simple groups, we have no idea how many, or what kind of, finite groups have C as their set of composition factors. So we are still very far away from solving the extension problem..

Also, the finite simple groups on our list are complicated! We still don't know everything we need to know about them (for example, we still haven't been able to classify all of their maximal subgroups). This brings us nicely to..

Ah, a quick aside just before we move on..

The so-called "2nd generation proof" of the Classification of Finite Simple Groups is currently being worked on, by Richard Lyons, Ron Solomon, and Warwick's own Inna Capdeboscq.

Ah, a quick aside just before we move on..

The so-called “2nd generation proof” of the Classification of Finite Simple Groups is currently being worked on, by Richard Lyons, Ron Solomon, and Warwick’s own Inna Capdeboscq.

The final proof will be more uniform in approach, and will be shorter. (The plan is a volume of 11 books, comprising about 3000 pages in total. Book 9 is almost ready..).

2. Asymptotic group theory

In this talk, we've focused mostly on deterministic type problems in finite group theory. That is, problems of the form: "Classify the finite groups with property $\mathcal{P}$..".

As we've seen, this is hard! It leads us to the branch of finite group theory called *Asymptotic group theory*.

In this talk, we've focused mostly on deterministic type problems in finite group theory. That is, problems of the form: "Classify the finite groups with property $\mathcal{P}$..".

As we've seen, this is hard! It leads us to the branch of finite group theory called *Asymptotic group theory*.

The philosophy behind asymptotic group theory is to say: "OK, we can't classify finite the finite groups with property $\mathcal{P}$, but can we say something about how many groups satisfy property $\mathcal{P}$? Or if we choose a finite group *at random* from a certain list, then how likely it is that the group we choose satisfies property $\mathcal{P}$?

In this talk, we've focused mostly on deterministic type problems in finite group theory. That is, problems of the form: "Classify the finite groups with property $\mathcal{P}$..".

As we've seen, this is hard! It leads us to the branch of finite group theory called *Asymptotic group theory*.

The philosophy behind asymptotic group theory is to say: "OK, we can't classify finite the finite groups with property $\mathcal{P}$, but can we say something about how many groups satisfy property $\mathcal{P}$? Or if we choose a finite group *at random* from a certain list, then how likely it is that the group we choose satisfies property $\mathcal{P}$?

We've see a little more of this later on when we look at the Restricted Burnside Problem. There, group theorists don't try to *classify* the d-generated finite groups with exponent n.. They just tried to count them.

In this talk, we've focused mostly on deterministic type problems in finite group theory. That is, problems of the form: "Classify the finite groups with property $\mathcal{P}$..".

As we've seen, this is hard! It leads us to the branch of finite group theory called *Asymptotic group theory*.

The philosophy behind asymptotic group theory is to say: "OK, we can't classify finite the finite groups with property $\mathcal{P}$, but can we say something about how many groups satisfy property $\mathcal{P}$? Or if we choose a finite group *at random* from a certain list, then how likely it is that the group we choose satisfies property $\mathcal{P}$?

We've see a little more of this later on when we look at the Restricted Burnside Problem. There, group theorists don't try to *classify* the d-generated finite groups with exponent n.. They just tried to count them.

A fact from earlier in the talk..

Earlier in the talk, we saw the number of groups of order 2^k, for $k \leq 10$.

A fact from earlier in the talk..

Earlier in the talk, we saw the number of groups of order 2^k, for $k \leq 10$.

$\|G\|$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

A fact from earlier in the talk..

Earlier in the talk, we saw the number of groups of order 2^k, for $k \leq 10$.

$\lvert G \rvert$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2. In fact, around 99.1% have order 2^{10}.

A fact from earlier in the talk..

Earlier in the talk, we saw the number of groups of order 2^k, for $k \leq 10$.

$\|G\|$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2. In fact, around 99.1% have order 2^{10}.

Conjecture (Erdös, 1965)

Let $f(n)$ be the number of isomorphism classes of finite groups of order n. If $n, x \in \mathbb{N}$ with $n \leq 2^x$, then $f(n) \leq f(2^x)$.

A fact from earlier in the talk..

Earlier in the talk, we saw the number of groups of order 2^k, for $k \leq 10$.

$\|G\|$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2. In fact, around 99.1% have order 2^{10}.

Conjecture (Erdös, 1965)

Let $f(n)$ be the number of isomorphism classes of finite groups of order n. If $n, x \in \mathbb{N}$ with $n \leq 2^x$, then $f(n) \leq f(2^x)$.

Conjecture (Pyber, 1990)

Let $f^*(n)$ be the number of isomorphism classes of finite groups of order at most n. Let $f_2^*(n)$ be the number of isomorphism classes of finite groups of 2-power order at most n. Then $f_2^*(n)/f^*(n) \to 1$ as $n \to \infty$. That is, a random finite group has order a power of 2.

A fact from earlier in the talk..

Earlier in the talk, we saw the number of groups of order 2^k, for $k \leq 10$.

$\|G\|$	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
#gps	1	2	5	14	57	267	2328	56092	10494213	49487365422

In total, there are roughly 49.5 billion groups of order at most 2047, and roughly 99.3% have order a power of 2. In fact, around 99.1% have order 2^{10}.

Conjecture (Erdös, 1965)

Let $f(n)$ be the number of isomorphism classes of finite groups of order n. If $n, x \in \mathbb{N}$ with $n \leq 2^x$, then $f(n) \leq f(2^x)$.

Conjecture (Pyber, 1990)

Let $f^*(n)$ be the number of isomorphism classes of finite groups of order at most n. Let $f_2^*(n)$ be the number of isomorphism classes of finite groups of 2-power order at most n. Then $f_2^*(n)/f^*(n) \to 1$ as $n \to \infty$. That is, a random finite group has order a power of 2.

Both of these conjectures are still open.

The number of isomorphism classes of finite groups of order at most n

For a positive integer n with prime factorisation

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \ (p_i \text{ distinct primes})$$

write $\mu(n) := \max\{a_i : 1 \leq i \leq n\}$. For example, $\mu(2^{10}23) = 10$.

The number of isomorphism classes of finite groups of order at most n

For a positive integer n with prime factorisation

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \ (p_i \text{ distinct primes})$$

write $\mu(n) := \max\{a_i : 1 \leq i \leq n\}$. For example, $\mu(2^{10}23) = 10$.

For a functions $g(n)$ and $h(n)$, the notation $h(n) = o(g(n))$ means that $h(n)/g(n) \to 0$ as $n \to \infty$. For example, $n^{5/3} = o(n^2)$.

The number of isomorphism classes of finite groups of order at most n

For a positive integer n with prime factorisation

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \text{ (} p_i \text{ distinct primes)}$$

write $\mu(n) := \max\{a_i : 1 \leq i \leq n\}$. For example, $\mu(2^{10}23) = 10$.

For a functions $g(n)$ and $h(n)$, the notation $h(n) = o(g(n))$ means that $h(n)/g(n) \to 0$ as $n \to \infty$. For example, $n^{5/3} = o(n^2)$.

In 1990, Pyber proved the following incredible result.

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$ and let $\mu := \mu(n)$. We have

$$f^*(n) \leq n^{\mu^2/27 + h(\mu)}$$

where $h(\mu) = o(\mu^2)$.

By work of Higman and Sims from the 1960s, the bound in the above theorem is "best possible".

More on Pyber's theorem

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$ *and let* $\mu := \mu(n)$*. We have* $f^*(n) \leq n^{\mu^2/27+h(\mu)}$ *where* $h(\mu) = o(\mu^2)$*.*

In order to make progress on Erdős' and Pyber's conjectures, one needs to find out more about the mysterious function h in the above theorem.

More on Pyber's theorem

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$ and let $\mu := \mu(n)$. We have $f^*(n) \leq n^{\mu^2/27+h(\mu)}$ where $h(\mu) = o(\mu^2)$.

In order to make progress on Erdős' and Pyber's conjectures, one needs to find out more about the mysterious function h in the above theorem.

In proving his theorem, one of three key steps that Pyber needed was a count on the total number of subgroups of the symmetric group S_n.

More on Pyber's theorem

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$ and let $\mu := \mu(n)$. We have $f^*(n) \leq n^{\mu^2/27+h(\mu)}$ where $h(\mu) = o(\mu^2)$.

In order to make progress on Erdős' and Pyber's conjectures, one needs to find out more about the mysterious function h in the above theorem.

In proving his theorem, one of three key steps that Pyber needed was a count on the total number of subgroups of the symmetric group S_n.

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{0.71n^2+h(n)}$, where $h(n) = o(n^2)$.

More on Pyber's theorem

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$ and let $\mu := \mu(n)$. We have $f^*(n) \leq n^{\mu^2/27+h(\mu)}$ where $h(\mu) = o(\mu^2)$.

In order to make progress on Erdős' and Pyber's conjectures, one needs to find out more about the mysterious function h in the above theorem.

In proving his theorem, one of three key steps that Pyber needed was a count on the total number of subgroups of the symmetric group S_n.

Theorem (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{0.71n^2+h(n)}$, where $h(n) = o(n^2)$.

He conjectured, however, that much more is true. (The following would be best possible).

Conjecture (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{n^2/16+h(n)}$, where $h(n) = o(n^2)$.

Pyber's conjecture

Conjecture (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{n^2/16+h(n)}$, where $h(n) = o(n^2)$.

Pyber's conjecture

Conjecture (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{n^2/16+h(n)}$, where $h(n) = o(n^2)$.

Pyber's conjecture is also heavily motivated by applications to:
(1) Galois theory (where one can count intermediate fields in a field extensions by counting subgroups of the associated Galois group);

Pyber's conjecture

Conjecture (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{n^2/16+h(n)}$, where $h(n) = o(n^2)$.

Pyber's conjecture is also heavily motivated by applications to:
(1) Galois theory (where one can count intermediate fields in a field extensions by counting subgroups of the associated Galois group);

(2) Graph theory: the number of vertex transitive graphs on n vertices is controlled by the number of (Certain) subgroups of S_n; and

Pyber's conjecture

Conjecture (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{n^2/16+h(n)}$, where $h(n) = o(n^2)$.

Pyber's conjecture is also heavily motivated by applications to:
(1) Galois theory (where one can count intermediate fields in a field extensions by counting subgroups of the associated Galois group);

(2) Graph theory: the number of vertex transitive graphs on n vertices is controlled by the number of (Certain) subgroups of S_n; and

(3) Topology: the number of conjugacy classes of subgroups of the fundamental group for certain path-connected topological spaces is equal to the number of coverings of that space.

Pyber's conjecture

Conjecture (Pyber, 1990)

Let $n \in \mathbb{N}$. The number of subgroups of the symmetric group S_n is at most $2^{n^2/16+h(n)}$, where $h(n) = o(n^2)$.

Pyber's conjecture is also heavily motivated by applications to:
(1) Galois theory (where one can count intermediate fields in a field extensions by counting subgroups of the associated Galois group);

(2) Graph theory: the number of vertex transitive graphs on n vertices is controlled by the number of (Certain) subgroups of S_n; and

(3) Topology: the number of conjugacy classes of subgroups of the fundamental group for certain path-connected topological spaces is equal to the number of coverings of that space.

Theorem (Roney-Dougal & T., 2023)

Pyber's conjecture holds. In fact, the number of subgroups of the symmetric group S_n is at most $2^{n^2/16+cn^{3/2}}$, where c is some absolute constant.

Probabilistic conjectures for permutation groups

Recall the probabilistic conjectures of Erdös and Pyber from earlier.

Conjecture (Pyber, 1990)

Let $f^*(n)$ be the number of isomorphism classes of finite groups of order at most n. Let $f_2^*(n)$ be the number of isomorphism classes of finite groups of 2-power order at most n. Then $f_2^*(n)/f^*(n) \to 1$ as $n \to \infty$. That is, a random finite group has order a power of 2.

Probabilistic conjectures for permutation groups

Recall the probabilistic conjectures of Erdös and Pyber from earlier.

Conjecture (Pyber, 1990)

Let $f^*(n)$ be the number of isomorphism classes of finite groups of order at most n. Let $f_2^*(n)$ be the number of isomorphism classes of finite groups of 2-power order at most n. Then $f_2^*(n)/f^*(n) \to 1$ as $n \to \infty$. That is, a random finite group has order a power of 2.

An analogue for permutation groups was proposed by Kantor.

Conjecture (Kantor, 1990)

Let $|\mathrm{Sub}(S_n)|$ and $|\mathrm{Sub}_2(S_n)|$ be the number of subgroups and 2-subgroups of S_n, respectively. Then $|\mathrm{Sub}_2(S_n)|/|\mathrm{Sub}(S_n)| \to 1$ as $n \to \infty$. That is, a random subgroup of S_n has order a power of 2.

Probabilistic conjectures for permutation groups

Recall the probabilistic conjectures of Erdös and Pyber from earlier.

Conjecture (Pyber, 1990)

Let $f^*(n)$ be the number of isomorphism classes of finite groups of order at most n. Let $f_2^*(n)$ be the number of isomorphism classes of finite groups of 2-power order at most n. Then $f_2^*(n)/f^*(n) \to 1$ as $n \to \infty$. That is, a random finite group has order a power of 2.

An analogue for permutation groups was proposed by Kantor.

Conjecture (Kantor, 1990)

Let $|\mathrm{Sub}(S_n)|$ and $|\mathrm{Sub}_2(S_n)|$ be the number of subgroups and 2-subgroups of S_n, respectively. Then $|\mathrm{Sub}_2(S_n)|/|\mathrm{Sub}(S_n)| \to 1$ as $n \to \infty$. That is, a random subgroup of S_n has order a power of 2.

Theorem (Roney-Dougal & T., 2024)

Kantor's conjecture is not true. Indeed, there exists an absolute constant $\epsilon > 0$ such that $|\mathrm{Sub}_2(S_n)|/|\mathrm{Sub}(S_n)| < 1 - \epsilon$ for all $n \in \mathbb{N}$.

Probabilistic conjectures for permutation groups

Recall the probabilistic conjectures of Erdös and Pyber from earlier.

Conjecture (Pyber, 1990)

Let $f^*(n)$ be the number of isomorphism classes of finite groups of order at most n. Let $f_2^*(n)$ be the number of isomorphism classes of finite groups of 2-power order at most n. Then $f_2^*(n)/f^*(n) \to 1$ as $n \to \infty$. That is, a random finite group has order a power of 2.

An analogue for permutation groups was proposed by Kantor.

Conjecture (Kantor, 1990)

Let $|\mathrm{Sub}(S_n)|$ and $|\mathrm{Sub}_2(S_n)|$ be the number of subgroups and 2-subgroups of S_n, respectively. Then $|\mathrm{Sub}_2(S_n)|/|\mathrm{Sub}(S_n)| \to 1$ as $n \to \infty$. That is, a random subgroup of S_n has order a power of 2.

Theorem (Roney-Dougal & T., 2024)

Kantor's conjecture is not true. Indeed, there exists an absolute constant $\epsilon > 0$ such that $|\mathrm{Sub}_2(S_n)|/|\mathrm{Sub}(S_n)| < 1 - \epsilon$ for all $n \in \mathbb{N}$.

One can take $\epsilon = 1/2^{16^2}$.

A number of questions arise from this theorem:

Question 1

Can we use this to make progress on the Erdős and Pyber conjectures?

A number of questions arise from this theorem:

Question 1

Can we use this to make progress on the Erdős and Pyber conjectures?

I think we still need better information on the constant c. At the moment, we can only show $c \leq 2^{16^2}$...

Question 2

Can we use similar techniques to count subgroups of other classes of finite (almost) simple groups? Or can we count certain types of subgroups of finite groups?

A number of questions arise from this theorem:

Question 1

Can we use this to make progress on the Erdős and Pyber conjectures?

I think we still need better information on the constant c. At the moment, we can only show $c \leq 2^{16^2}$...

Question 2

Can we use similar techniques to count subgroups of other classes of finite (almost) simple groups? Or can we count certain types of subgroups of finite groups?

The final part of Question 2 is not "just for the sake of it". There is very practical motivation..

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

An easy method

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

An easy method

Step 1: Choose a set X of generators for G_1 of size at most $\log |G_1| = \log n$.

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

An easy method

Step 1: Choose a set X of generators for G_1 of size at most $\log |G_1| = \log n$.

Step 2: Write down all maps $f : X \to G_2$. Use the multiplication table for G_2 to check which ones (if any) are isomorphisms.

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

An easy method

Step 1: Choose a set X of generators for G_1 of size at most $\log |G_1| = \log n$.

Step 2: Write down all maps $f : X \to G_2$. Use the multiplication table for G_2 to check which ones (if any) are isomorphisms.

In total, this takes time $n^{\log n + o(\log n)}$..

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

An easy method

Step 1: Choose a set X of generators for G_1 of size at most $\log |G_1| = \log n$.

Step 2: Write down all maps $f : X \to G_2$. Use the multiplication table for G_2 to check which ones (if any) are isomorphisms.

In total, this takes time $n^{\log n + o(\log n)}$..

And we still can't do much better! The best general result to date is to due to Rosenbaum (2013), who showed that one can solve GrpI in time $n^{0.5 \log n + o(\log n)}$.

The Group Isomorphism Problem

The *Group Isomorphism Problem* (henceforth abbreviated to GrpI) is the decision problem for determining whether or not two groups G_1 and G_2 given by their multiplication tables are isomorphic.

The Group Isomorphism Problem (version we usually study)

Can we come up with an algorithm such that, given the multiplication tables of two groups G_1 and G_2 of order n as input, a computer can decide in a time which is polynomial in n, whether or not $G_1 \cong G_2$?

An easy method

Step 1: Choose a set X of generators for G_1 of size at most $\log |G_1| = \log n$.

Step 2: Write down all maps $f : X \to G_2$. Use the multiplication table for G_2 to check which ones (if any) are isomorphisms.

In total, this takes time $n^{\log n + o(\log n)}$..

And we still can't do much better! The best general result to date is to due to Rosenbaum (2013), who showed that one can solve GrpI in time $n^{0.5 \log n + o(\log n)}$.

What has this got to with counting subgroups of finite groups?!

An intriguing new approach due to Gowers shows that an improved understanding of subgroup enumeration could lead to remarkable progress in GrpI.

The idea is as follows: For finite groups G and X, let $\mathrm{Sub}_{\cong X}(G)$ be the set of subgroups H of G with $H \cong X$. For $n \in \mathbb{N}$, let $k(n)$ be the smallest positive integer such that for any two finite groups G_1 and G_2 of order n, we have $G_1 \cong G_2$ if and only if $|\mathrm{Sub}_{\cong X}(G_1)| = |\mathrm{Sub}_{\cong X}(G_2)|$ for all $k(n)$-generated finite groups X. Then the GrpI can be solved in time $n^{k(n)}$.

What has this got to with counting subgroups of finite groups?!

An intriguing new approach due to Gowers shows that an improved understanding of subgroup enumeration could lead to remarkable progress in GrpI.

The idea is as follows: For finite groups G and X, let $\mathrm{Sub}_{\cong X}(G)$ be the set of subgroups H of G with $H \cong X$. For $n \in \mathbb{N}$, let $k(n)$ be the smallest positive integer such that for any two finite groups G_1 and G_2 of order n, we have $G_1 \cong G_2$ if and only if $|\mathrm{Sub}_{\cong X}(G_1)| = |\mathrm{Sub}_{\cong X}(G_2)|$ for all $k(n)$-generated finite groups X. Then the GrpI can be solved in time $n^{k(n)}$.

Gowers' $k(n)$ problem

Can we come up with upper bounds on $k(n)$, in terms of n?

What has this got to with counting subgroups of finite groups?!

An intriguing new approach due to Gowers shows that an improved understanding of subgroup enumeration could lead to remarkable progress in GrpI.

The idea is as follows: For finite groups G and X, let $\mathrm{Sub}_{\cong X}(G)$ be the set of subgroups H of G with $H \cong X$. For $n \in \mathbb{N}$, let $k(n)$ be the smallest positive integer such that for any two finite groups G_1 and G_2 of order n, we have $G_1 \cong G_2$ if and only if $|\mathrm{Sub}_{\cong X}(G_1)| = |\mathrm{Sub}_{\cong X}(G_2)|$ for all $k(n)$-generated finite groups X. Then the GrpI can be solved in time $n^{k(n)}$.

Gowers' $k(n)$ problem

Can we come up with upper bounds on $k(n)$, in terms of n?

All we know at the moment is that $k(n) \leq \log n$..

3. Burnside's problems

In mathematical terms, Group Theory is quite a young subject (Galois first defined a group in 1830, though Euler and Lagrange had already done some work on groups, under a different name, in the 18th century).

In mathematical terms, Group Theory is quite a young subject (Galois first defined a group in 1830, though Euler and Lagrange had already done some work on groups, under a different name, in the 18th century).

By the late 1800s, we knew very little about abstract group theory. One of the most influential early group theorists was William Burnside.

In mathematical terms, Group Theory is quite a young subject (Galois first defined a group in 1830, though Euler and Lagrange had already done some work on groups, under a different name, in the 18th century).

By the late 1800s, we knew very little about abstract group theory. One of the most influential early group theorists was William Burnside.

In 1901, Burnside asked the following famous question.

Burnside's problem

Let G be a group which can be generated by d elements (G is said to be *d-generated* in this case), and such that $g^n = 1_G$ for all $g \in G$ (G is said to have *exponent* n in this case). Is G necessarily finite?

Unpacking Burnside's problem

Burnside's problem

Let G be a group which can be generated by d elements (G is said to be *d-generated* in this case), and such that $g^n = 1_G$ for all $g \in G$ (G is said to have *exponent* n in this case). Is G necessarily finite?

Definition

Let G be a group, and let A be a non-empty subset of G. The *subgroup of G generated by A*, written $\langle A \rangle$, is defined to be

$$\langle A \rangle := \{a_1^{\epsilon_1} \ldots a_m^{\epsilon_m} : m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}.$$

Unpacking Burnside's problem

Burnside's problem

Let G be a group which can be generated by d elements (G is said to be *d-generated* in this case), and such that $g^n = 1_G$ for all $g \in G$ (G is said to have *exponent n* in this case). Is G necessarily finite?

Definition

Let G be a group, and let A be a non-empty subset of G. The *subgroup of G generated by A*, written $\langle A \rangle$, is defined to be

$$\langle A \rangle := \{a_1^{\epsilon_1} \dots a_m^{\epsilon_m} : m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}.$$

So Burnside's problems says that if G is a group, there exists $A \subseteq G$ of size d such that every element can be written as a product of powers of elements of A, and every element of G has order at most n, then is G finite? Or, more informally, if G "operationally" finite, then is G finite?

Unpacking Burnside's problem

Burnside's problem

Let G be a group which can be generated by d elements (G is said to be *d-generated* in this case), and such that $g^n = 1_G$ for all $g \in G$ (G is said to have *exponent n* in this case). Is G necessarily finite?

Definition

Let G be a group, and let A be a non-empty subset of G. The *subgroup of G generated by A*, written $\langle A \rangle$, is defined to be

$$\langle A \rangle := \{a_1^{\epsilon_1} \dots a_m^{\epsilon_m} : m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}.$$

So Burnside's problems says that if G is a group, there exists $A \subseteq G$ of size d such that every element can be written as a product of powers of elements of A, and every element of G has order at most n, then is G finite? Or, more informally, if G "operationally" finite, then is G finite?

Does this seem like a reasonable question?

Unpacking Burnside's problem

Burnside's problem

Let G be a group which can be generated by d elements (G is said to be *d-generated* in this case), and such that $g^n = 1_G$ for all $g \in G$ (G is said to have *exponent n* in this case). Is G necessarily finite?

Definition

Let G be a group, and let A be a non-empty subset of G. The *subgroup of G generated by A*, written $\langle A \rangle$, is defined to be

$$\langle A \rangle := \{a_1^{\epsilon_1} \dots a_m^{\epsilon_m} : m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}.$$

So Burnside's problems says that if G is a group, there exists $A \subseteq G$ of size d such that every element can be written as a product of powers of elements of A, and every element of G has order at most n, then is G finite? Or, more informally, if G "operationally" finite, then is G finite?

Does this seem like a reasonable question?

Example 1 Suppose that G, d and n are as in Burnside's question, and $n = 2$ (i.e. G is a d-generated group in which $g^2 = 1_G$ for all $g \in G$).

Then $g = g^{-1}$ for all $g \in G$, so we have

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

for all $a, b \in G$.

Then $g = g^{-1}$ for all $g \in G$, so we have

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

for all $a, b \in G$.

Thus, G is abelian. Hence, writing $A = \{x_1, \ldots, x_d\}$, we have

$$\begin{aligned} |G| = |\langle A \rangle| &= |\{a_1^{\epsilon_1} \ldots a_m^{\epsilon_m} : m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}| \\ &= |\{x_1^{e_1} \ldots x_d^{e_d} : e_i \in \{0, 1\}\}| \leq 2^d. \end{aligned}$$

Then $g = g^{-1}$ for all $g \in G$, so we have

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

for all $a, b \in G$.

Thus, G is abelian. Hence, writing $A = \{x_1, \ldots, x_d\}$, we have

$$\begin{aligned} |G| = |\langle A \rangle| &= |\{a_1^{\epsilon_1} \ldots a_m^{\epsilon_m} \, : \, m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}| \\ &= |\{x_1^{e_1} \ldots x_d^{e_d} \, : \, e_i \in \{0, 1\}\}| \leq 2^d. \end{aligned}$$

So Burnside's problem has an affirmative answer in the case $n = 2$!

Then $g = g^{-1}$ for all $g \in G$, so we have

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

for all $a, b \in G$.

Thus, G is abelian. Hence, writing $A = \{x_1, \dots, x_d\}$, we have

$$\begin{aligned} |G| = |\langle A \rangle| &= |\{a_1^{\epsilon_1} \dots a_m^{\epsilon_m} \,:\, m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}| \\ &= |\{x_1^{e_1} \dots x_d^{e_d} \,:\, e_i \in \{0, 1\}\}| \leq 2^d. \end{aligned}$$

So Burnside's problem has an affirmative answer in the case $n = 2$!

Example 2 Suppose that G, d and n are as in Burnside's question, and $n = 3$ (i.e. G is a d-generated group in which $g^3 = 1_G$ for all $g \in G$).

Then $g = g^{-1}$ for all $g \in G$, so we have

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

for all $a, b \in G$.

Thus, G is abelian. Hence, writing $A = \{x_1, \ldots, x_d\}$, we have

$$\begin{aligned} |G| = |\langle A \rangle| &= |\{a_1^{\epsilon_1} \ldots a_m^{\epsilon_m} \,:\, m \in \mathbb{N}, a_i \in A, \epsilon_i \in \mathbb{Z}\}| \\ &= |\{x_1^{e_1} \ldots x_d^{e_d} \,:\, e_i \in \{0,1\}\}| \leq 2^d. \end{aligned}$$

So Burnside's problem has an affirmative answer in the case $n = 2$!

Example 2 Suppose that G, d and n are as in Burnside's question, and $n = 3$ (i.e. G is a d-generated group in which $g^3 = 1_G$ for all $g \in G$).

The same approach won't work (there are examples of finite groups of exponent 3 which are not abelian). But is there anything we can do?

Yes! Claim: Let G be a group of exponent 3. Then G is "almost abelian". More precisely, a commutes with $a^b := b^{-1}ab$ for all $a, b \in G$.

Yes! Claim: Let G be a group of exponent 3. Then G is "almost abelian". More precisely, a commutes with $a^b := b^{-1}ab$ for all $a, b \in G$.

Proof of claim: Let G be as in the statement, and let a and b be elements of G. Then we have

$$\begin{aligned} 1_G = (ba)^3 &= bababa \\ &= b(b^2b^{-2})a(b^2b^{-2})baba \\ &= b^3(b^{-2}ab^2)(b^{-2}b)aba \\ &= (bab^{-1})(b^{-1}ab)a \qquad \text{since } b^3 = 1_G\text{, and hence } b = b^{-2}. \\ &= (bab^{-1})(b^2ab^{-2})a. \end{aligned}$$

We therefore have $a^{-1} = a^{b^{-1}}a^b$. Replacing b by b^{-1} gives $a^{-1} = a^b a^{b^{-1}}$. Thus,

$$a^{b^{-1}}a^b = a^b a^{b^{-1}} \text{ for all } a, b \in G.$$

So raising both sides to the b^2 yields:

$$a^b a = aa^b \text{ for all } a, b \in G.$$

The point of the previous claim is that if G is a group of exponent 3 which can generated by d elements (say $a_1, \ldots, a_d$), then the group

$$N := \langle a_d^b : b \in G \rangle$$

is abelian, hence isomorphic to C_3^m for some m (by the same argument as used in Example 1). Since $N \trianglelefteq G$ and G/N can be generated by $\langle a_1 N, \ldots, a_{d-1} N \rangle$, an easy inductive argument shows that G is finite.

The point of the previous claim is that if G is a group of exponent 3 which can generated by d elements (say $a_1, \ldots, a_d$), then the group

$$N := \langle a_d^b : b \in G \rangle$$

is abelian, hence isomorphic to C_3^m for some m (by the same argument as used in Example 1). Since $N \trianglelefteq G$ and G/N can be generated by $\langle a_1 N, \ldots, a_{d-1} N \rangle$, an easy inductive argument shows that G is finite.

So in summary, recalling:

Burnside's problem

Let G be a d-generated group of exponent n. Is G necessarily finite?

- The case $n = 2$ is easy;

The point of the previous claim is that if G is a group of exponent 3 which can generated by d elements (say $a_1, \ldots, a_d$), then the group

$$N := \langle a_d^b : b \in G \rangle$$

is abelian, hence isomorphic to C_3^m for some m (by the same argument as used in Example 1). Since $N \trianglelefteq G$ and G/N can be generated by $\langle a_1 N, \ldots, a_{d-1} N \rangle$, an easy inductive argument shows that G is finite.

So in summary, recalling:

Burnside's problem

Let G be a d-generated group of exponent n. Is G necessarily finite?

- The case $n = 2$ is easy;
- the case $n = 3$ is easy-ish;

The point of the previous claim is that if G is a group of exponent 3 which can generated by d elements (say $a_1, \ldots, a_d$), then the group

$$N := \langle a_d^b : b \in G \rangle$$

is abelian, hence isomorphic to C_3^m for some m (by the same argument as used in Example 1). Since $N \trianglelefteq G$ and G/N can be generated by $\langle a_1 N, \ldots, a_{d-1} N \rangle$, an easy inductive argument shows that G is finite.

So in summary, recalling:

Burnside's problem

Let G be a d-generated group of exponent n. Is G necessarily finite?

- The case $n = 2$ is easy;
- the case $n = 3$ is easy-ish;
- the case $n = 4$ is easy-ish (done by Sanov in 1940);

The point of the previous claim is that if G is a group of exponent 3 which can generated by d elements (say $a_1, \ldots, a_d$), then the group

$$N := \langle a_d^b : b \in G \rangle$$

is abelian, hence isomorphic to C_3^m for some m (by the same argument as used in Example 1). Since $N \trianglelefteq G$ and G/N can be generated by $\langle a_1 N, \ldots, a_{d-1} N \rangle$, an easy inductive argument shows that G is finite.

So in summary, recalling:

Burnside's problem

Let G be a d-generated group of exponent n. Is G necessarily finite?

- The case $n = 2$ is easy;
- the case $n = 3$ is easy-ish;
- the case $n = 4$ is easy-ish (done by Sanov in 1940);
- What about the case $n = 5$?

The point of the previous claim is that if G is a group of exponent 3 which can generated by d elements (say $a_1, \ldots, a_d$), then the group

$$N := \langle a_d^b : b \in G \rangle$$

is abelian, hence isomorphic to C_3^m for some m (by the same argument as used in Example 1). Since $N \trianglelefteq G$ and G/N can be generated by $\langle a_1 N, \ldots, a_{d-1} N \rangle$, an easy inductive argument shows that G is finite.

So in summary, recalling:

Burnside's problem

Let G be a d-generated group of exponent n. Is G necessarily finite?

- The case $n = 2$ is easy;
- the case $n = 3$ is easy-ish;
- the case $n = 4$ is easy-ish (done by Sanov in 1940);
- What about the case $n = 5$?

NOBODY KNOWS..

Burnside's problem in exponent 5

Burnside's problem in exponent 5 is notoriously difficult: we know almost nothing about the problem in this case.

Even if we restrict to the case $d = 2$, we still have no idea what happens.

Burnside's problem in exponent 5

Burnside's problem in exponent 5 is notoriously difficult: we know almost nothing about the problem in this case.

Even if we restrict to the case $d = 2$, we still have no idea what happens.

Burnside's $B(2,5)$ problem (open)

Let G be a group which can be generated by 2 elements, and such that $g^5 = 1_G$ for all $g \in G$. Is G necessarily finite?

Burnside's problem in exponent 5

Burnside's problem in exponent 5 is notoriously difficult: we know almost nothing about the problem in this case.

Even if we restrict to the case $d = 2$, we still have no idea what happens.

Burnside's $B(2,5)$ problem (open)

Let G be a group which can be generated by 2 elements, and such that $g^5 = 1_G$ for all $g \in G$. Is G necessarily finite?

Despite this obstacle, a huge breakthrough was made concerning Burnside's problem in 1968.

Burnside's problem in exponent 5

Burnside's problem in exponent 5 is notoriously difficult: we know almost nothing about the problem in this case.

Even if we restrict to the case $d = 2$, we still have no idea what happens.

Burnside's $B(2,5)$ problem (open)

Let G be a group which can be generated by 2 elements, and such that $g^5 = 1_G$ for all $g \in G$. Is G necessarily finite?

Despite this obstacle, a huge breakthrough was made concerning Burnside's problem in 1968.

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Burnside's problem is NO.

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Notes:

1. The lower bound in the theorem was improved to 101 by Adian in 2015. We still have no idea what happens between 5 and 101 (apart from 6 – Marshall Hall proved in 1956 that G is finite in this case).

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Notes:

1. The lower bound in the theorem was improved to 101 by Adian in 2015. We still have no idea what happens between 5 and 101 (apart from 6 – Marshall Hall proved in 1956 that G is finite in this case).
2. A similar result holds for even integers n, and is due to Ivanov (1994).

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Notes:

1. The lower bound in the theorem was improved to 101 by Adian in 2015. We still have no idea what happens between 5 and 101 (apart from 6 – Marshall Hall proved in 1956 that G is finite in this case).
2. A similar result holds for even integers n, and is due to Ivanov (1994).
3. Olshanskii provided another (incredible) counterexample to Burnside's problem in 1979: For a prime p, he constructed infinite simple groups $T(p)$ such that:

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Notes:

1. The lower bound in the theorem was improved to 101 by Adian in 2015. We still have no idea what happens between 5 and 101 (apart from 6 – Marshall Hall proved in 1956 that G is finite in this case).
2. A similar result holds for even integers n, and is due to Ivanov (1994).
3. Olshanskii provided another (incredible) counterexample to Burnside's problem in 1979: For a prime p, he constructed infinite simple groups $T(p)$ such that:
   - $T(p)$ can be generated by 2 elements; and

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Notes:

1. The lower bound in the theorem was improved to 101 by Adian in 2015. We still have no idea what happens between 5 and 101 (apart from 6 – Marshall Hall proved in 1956 that G is finite in this case).
2. A similar result holds for even integers n, and is due to Ivanov (1994).
3. Olshanskii provided another (incredible) counterexample to Burnside's problem in 1979: For a prime p, he constructed infinite simple groups $T(p)$ such that:
   - $T(p)$ can be generated by 2 elements; and
   - Every nontrivial proper subgroup of $T(p)$ is finite of order p.

Theorem (Adian and Novikov, 1968)

For every odd number n with $n > 4381$, there exist infinite, finitely generated groups of exponent n. Thus, the answer to Bursnide's problem is NO.

Notes:

1. The lower bound in the theorem was improved to 101 by Adian in 2015. We still have no idea what happens between 5 and 101 (apart from 6 – Marshall Hall proved in 1956 that G is finite in this case).
2. A similar result holds for even integers n, and is due to Ivanov (1994).
3. Olshanskii provided another (incredible) counterexample to Burnside's problem in 1979: For a prime p, he constructed infinite simple groups $T(p)$ such that:
   - $T(p)$ can be generated by 2 elements; and
   - Every nontrivial proper subgroup of $T(p)$ is finite of order p.

   These are called *Tarski Monsters*, and they exist for every prime $p > 10^{75}$.

These examples (and the proofs within) show that Burnside's problem is very difficult in general.

These examples (and the proofs within) show that Burnside's problem is very difficult in general.

Because of this difficulty, and in general the lack of progress made in the first 30 years after the statement of Burnside's problem, mathematicians started to ask a weaker question in the 1930s. This became known as the *Restricted Burnside problem*:

These examples (and the proofs within) show that Burnside's problem is very difficult in general.

Because of this difficulty, and in general the lack of progress made in the first 30 years after the statement of Burnside's problem, mathematicians started to ask a weaker question in the 1930s. This became known as the *Restricted Burnside problem*:

Restricted Burnside problem

Fix $d, n \in \mathbb{N}$. Are there are only finitely many finite d-generated groups G of exponent n?

These examples (and the proofs within) show that Burnside's problem is very difficult in general.

Because of this difficulty, and in general the lack of progress made in the first 30 years after the statement of Burnside's problem, mathematicians started to ask a weaker question in the 1930s. This became known as the *Restricted Burnside problem*:

Restricted Burnside problem

Fix $d, n \in \mathbb{N}$. Are there are only finitely many finite d-generated groups G of exponent n?

A famous theorem of Hall & Higman (1956) shows* that the restricted Burnside problem has an affirmative answer if and only if it has an affirmative answer in the case where n is a prime power.

These examples (and the proofs within) show that Burnside's problem is very difficult in general.

Because of this difficulty, and in general the lack of progress made in the first 30 years after the statement of Burnside's problem, mathematicians started to ask a weaker question in the 1930s. This became known as the *Restricted Burnside problem*:

Restricted Burnside problem

Fix $d, n \in \mathbb{N}$. Are there are only finitely many finite d-generated groups G of exponent n?

A famous theorem of Hall & Higman (1956) shows* that the restricted Burnside problem has an affirmative answer if and only if it has an affirmative answer in the case where n is a prime power.

*There was one (pretty huge) caveat to the Hall-Higman theorem: they prove that their result holds as long as, for each nonabelian simple group S: (1) S can be generated by 2 elements; and (2) the only nonabelian composition factor in $\mathrm{Aut}(S)$ is S itself.

These examples (and the proofs within) show that Burnside's problem is very difficult in general.

Because of this difficulty, and in general the lack of progress made in the first 30 years after the statement of Burnside's problem, mathematicians started to ask a weaker question in the 1930s. This became known as the *Restricted Burnside problem*:

Restricted Burnside problem

Fix $d, n \in \mathbb{N}$. Are there are only finitely many finite d-generated groups G of exponent n?

A famous theorem of Hall & Higman (1956) shows* that the restricted Burnside problem has an affirmative answer if and only if it has an affirmative answer in the case where n is a prime power.

*There was one (pretty huge) caveat to the Hall-Higman theorem: they prove that their result holds as long as, for each nonabelian simple group S: (1) S can be generated by 2 elements; and (2) the only nonabelian composition factor in $\mathrm{Aut}(S)$ is S itself. We only know these 2 things hold because of CFSG, announced 27 years later!

The Restricted Burnside problem

With the Hall–Higman reduction in mind, group theorists began working furiously on the restricted Burnside problem in prime power exponent. This allows one to assume that the group G one is working in is a finite p-group, for some prime p (i.e. G has p-power order).

The Restricted Burnside problem

With the Hall–Higman reduction in mind, group theorists began working furiously on the restricted Burnside problem in prime power exponent. This allows one to assume that the group G one is working in is a finite p-group, for some prime p (i.e. G has p-power order).

The first significant breakthrough came from Kostrikin in 1959.

Theorem (Kostrikin, 1959)

Fix $d \in \mathbb{N}$ and a prime p. There are only finitely many finite d-generated groups G of exponent p. That is, the Restricted Burnside problem has a positive solution for prime exponents.

The Restricted Burnside problem

With the Hall–Higman reduction in mind, group theorists began working furiously on the restricted Burnside problem in prime power exponent. This allows one to assume that the group G one is working in is a finite p-group, for some prime p (i.e. G has p-power order).

The first significant breakthrough came from Kostrikin in 1959.

Theorem (Kostrikin, 1959)

Fix $d \in \mathbb{N}$ and a prime p. There are only finitely many finite d-generated groups G of exponent p. That is, the Restricted Burnside problem has a positive solution for prime exponents.

Kostrikin's idea used an intriguing connection between finite groups of p-power order, and *Lie algebras* (on which Warwick's Adam Thomas is one of the world's foremost experts!)

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot, \cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot,\cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

(b) $[\cdot,\cdot] : L \times L \to L$ is a bilinear map. That is, it satisfies $[v + w, u] = [v, u] + [w, u]$ and $[\lambda v, u] = \lambda[v, u]$ for all $\lambda \in \mathbb{F}$; and also the analogous linearity relations in the second coordinate.

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot, \cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

(b) $[\cdot, \cdot] : L \times L \to L$ is a bilinear map. That is, it satisfies $[v + w, u] = [v, u] + [w, u]$ and $[\lambda v, u] = \lambda[v, u]$ for all $\lambda \in \mathbb{F}$; and also the analogous linearity relations in the second coordinate.

(c) $[v, v] = 0$ for all $v \in L$.

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot,\cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

(b) $[\cdot,\cdot] : L \times L \to L$ is a bilinear map. That is, it satisfies $[v + w, u] = [v, u] + [w, u]$ and $[\lambda v, u] = \lambda[v, u]$ for all $\lambda \in \mathbb{F}$; and also the analogous linearity relations in the second coordinate.

(c) $[v, v] = 0$ for all $v \in L$.

(d) The *Jacobi identity* $[u, [v, w]] + [w, [u, v]] + [v, [w, u]] = 0$ holds for all $u, v, w \in L$.

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot,\cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

(b) $[\cdot,\cdot] : L \times L \to L$ is a bilinear map. That is, it satisfies $[v+w, u] = [v, u] + [w, u]$ and $[\lambda v, u] = \lambda[v, u]$ for all $\lambda \in \mathbb{F}$; and also the analogous linearity relations in the second coordinate.

(c) $[v, v] = 0$ for all $v \in L$.

(d) The *Jacobi identity* $[u, [v, w]] + [w, [u, v]] + [v, [w, u]] = 0$ holds for all $u, v, w \in L$.

The standard example is $L := M_n(\mathbb{F})$, the set of $(n \times n)$-matrices over $\mathbb{F}$, where $[A, B] := AB - BA$.

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot,\cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

(b) $[\cdot,\cdot] : L \times L \to L$ is a bilinear map. That is, it satisfies $[v+w,u] = [v,u] + [w,u]$ and $[\lambda v, u] = \lambda[v,u]$ for all $\lambda \in \mathbb{F}$; and also the analogous linearity relations in the second coordinate.

(c) $[v,v] = 0$ for all $v \in L$.

(d) The *Jacobi identity* $[u,[v,w]] + [w,[u,v]] + [v,[w,u]] = 0$ holds for all $u,v,w \in L$.

The standard example is $L := M_n(\mathbb{F})$, the set of $(n \times n)$-matrices over $\mathbb{F}$, where $[A,B] := AB - BA$.

But what has this got to do with finite p-groups?!

Lie algebras and finite p-groups

Definition

Let $\mathbb{F}$ be a field. A *Lie algebra over* $\mathbb{F}$ is a pair $(L, [\cdot, \cdot])$ where

(a) L is a vector space over $\mathbb{F}$;

(b) $[\cdot, \cdot] : L \times L \to L$ is a bilinear map. That is, it satisfies $[v + w, u] = [v, u] + [w, u]$ and $[\lambda v, u] = \lambda[v, u]$ for all $\lambda \in \mathbb{F}$; and also the analogous linearity relations in the second coordinate.

(c) $[v, v] = 0$ for all $v \in L$.

(d) The *Jacobi identity* $[u, [v, w]] + [w, [u, v]] + [v, [w, u]] = 0$ holds for all $u, v, w \in L$.

The standard example is $L := M_n(\mathbb{F})$, the set of $(n \times n)$-matrices over $\mathbb{F}$, where $[A, B] := AB - BA$.

But what has this got to do with finite p-groups?!

The connection

Let G be a finite group of exponent p (i.e. $g^p = 1_G$ for all $g \in G$). The *commutator subgroup* $\gamma_2(G) := [G, G]$ is defined by

$$[G, G] := \langle [g, h] : g, h \in G \rangle$$

where $[g, h] := ghg^{-1}h^{-1}$. It's main property is that $G/[G, G]$ is abelian.

The connection

Let G be a finite group of exponent p (i.e. $g^p = 1_G$ for all $g \in G$). The *commutator subgroup* $\gamma_2(G) := [G, G]$ is defined by

$$[G, G] := \langle [g, h] : g, h \in G \rangle$$

where $[g, h] := ghg^{-1}h^{-1}$. It's main property is that $G/[G, G]$ is abelian.

Since $G/[G, G]$ is abelian, and G has exponent p, we have that $G/[G, G] \cong (\mathbb{Z}/p\mathbb{Z})^n$. That is, $G/[G, G]$ is a vector space (of dimension n) over the field $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$.

The connection

Let G be a finite group of exponent p (i.e. $g^p = 1_G$ for all $g \in G$). The *commutator subgroup* $\gamma_2(G) := [G, G]$ is defined by

$$[G, G] := \langle [g, h] : g, h \in G \rangle$$

where $[g, h] := ghg^{-1}h^{-1}$. It's main property is that $G/[G, G]$ is abelian.

Since $G/[G, G]$ is abelian, and G has exponent p, we have that $G/[G, G] \cong (\mathbb{Z}/p\mathbb{Z})^n$. That is, $G/[G, G]$ is a vector space (of dimension n) over the field $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$.

We now define $\gamma_1(G) := G$, and for $i \geq 2$,

$$\gamma_i(G) := \langle [x, g] : x \in \gamma_{i-1}(G), g \in G \rangle.$$

It is not hard to show that $\gamma_{c+1}(G) = \{1_G\}$ for some $c \in \mathbb{N}$.

The connection

Let G be a finite group of exponent p (i.e. $g^p = 1_G$ for all $g \in G$). The *commutator subgroup* $\gamma_2(G) := [G, G]$ is defined by

$$[G, G] := \langle [g, h] : g, h \in G \rangle$$

where $[g, h] := ghg^{-1}h^{-1}$. It's main property is that $G/[G, G]$ is abelian.

Since $G/[G, G]$ is abelian, and G has exponent p, we have that $G/[G, G] \cong (\mathbb{Z}/p\mathbb{Z})^n$. That is, $G/[G, G]$ is a vector space (of dimension n) over the field $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$.

We now define $\gamma_1(G) := G$, and for $i \geq 2$,

$$\gamma_i(G) := \langle [x, g] : x \in \gamma_{i-1}(G), g \in G \rangle.$$

It is not hard to show that $\gamma_{c+1}(G) = \{1_G\}$ for some $c \in \mathbb{N}$.

We then define
$L(G) := \gamma_1(G)/\gamma_2(G) \oplus \gamma_2(G)/\gamma_3(G) \oplus \ldots \oplus \gamma_n(G)/\gamma_{c+1}(G)$;

The connection

Let G be a finite group of exponent p (i.e. $g^p = 1_G$ for all $g \in G$). The *commutator subgroup* $\gamma_2(G) := [G, G]$ is defined by

$$[G, G] := \langle [g, h] : g, h \in G \rangle$$

where $[g, h] := ghg^{-1}h^{-1}$. It's main property is that $G/[G, G]$ is abelian.

Since $G/[G, G]$ is abelian, and G has exponent p, we have that $G/[G, G] \cong (\mathbb{Z}/p\mathbb{Z})^n$. That is, $G/[G, G]$ is a vector space (of dimension n) over the field $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$.

We now define $\gamma_1(G) := G$, and for $i \geq 2$,

$$\gamma_i(G) := \langle [x, g] : x \in \gamma_{i-1}(G), g \in G \rangle.$$

It is not hard to show that $\gamma_{c+1}(G) = \{1_G\}$ for some $c \in \mathbb{N}$.

We then define
$L(G) := \gamma_1(G)/\gamma_2(G) \oplus \gamma_2(G)/\gamma_3(G) \oplus \ldots \oplus \gamma_n(G)/\gamma_{c+1}(G)$;and we set

$$[v\gamma_i(G), w\gamma_j(G)] := [v, w]\gamma_{i+j \pmod{n}}(G).$$

Extending this operation linearly to all of $L(G)$, we get a Lie algebra, called the *Lie algebra associated to* G.

Extending this operation linearly to all of $L(G)$, we get a Lie algebra, called the *Lie algebra associated to G.*

In much the same way that Galois theory uses Group Theory to solve problems in Number Theory, Kostrikin used this connection between finite p-groups of exponent p and Lie algebras over $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$ to make the extraordinary breakthrough on the Restricted Burnside problem mentioned above.

Extending this operation linearly to all of $L(G)$, we get a Lie algebra, called the *Lie algebra associated to* G.

In much the same way that Galois theory uses Group Theory to solve problems in Number Theory, Kostrikin used this connection between finite p-groups of exponent p and Lie algebras over $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$ to make the extraordinary breakthrough on the Restricted Burnside problem mentioned above.

The case of general prime power exponent $d := p^m$ was done by Zelmanov in the late 1980s. He used a similar connection to the above, but needed to work with *Lie rings* rather than Lie algebras, as $\mathbb{Z}/p^m\mathbb{Z}$ is a field if and only if $m = 1$.

Extending this operation linearly to all of $L(G)$, we get a Lie algebra, called the *Lie algebra associated to G.*

In much the same way that Galois theory uses Group Theory to solve problems in Number Theory, Kostrikin used this connection between finite p-groups of exponent p and Lie algebras over $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$ to make the extraordinary breakthrough on the Restricted Burnside problem mentioned above.

The case of general prime power exponent $d := p^m$ was done by Zelmanov in the late 1980s. He used a similar connection to the above, but needed to work with *Lie rings* rather than Lie algebras, as $\mathbb{Z}/p^m\mathbb{Z}$ is a field if and only if $m = 1$.

In 1994, Zelmanov was awarded the Fields medal for his work.

Conclusion

Finite group theorists focus on two types of problems:

1. *Classification* type problems (e.g. the CFSG); and

Conclusion

Finite group theorists focus on two types of problems:

1. *Classification* type problems (e.g. the CFSG); and
2. *Asymptotic* type problems (e.g. counting subgroups of finite groups; asking what a random finite group looks like).

Conclusion

Finite group theorists focus on two types of problems:

1. *Classification* type problems (e.g. the CFSG); and
2. *Asymptotic* type problems (e.g. counting subgroups of finite groups; asking what a random finite group looks like).

Although the first of these is *a priori* harder, classification problems can be restrictive, and don't always lead to progress in the asymptotic problems that are needed for work on things like the Group Isomorphism Problem, and Galois theoretic problems.

Conclusion

Finite group theorists focus on two types of problems:

1. *Classification* type problems (e.g. the CFSG); and
2. *Asymptotic* type problems (e.g. counting subgroups of finite groups; asking what a random finite group looks like).

Although the first of these is *a priori* harder, classification problems can be restrictive, and don't always lead to progress in the asymptotic problems that are needed for work on things like the Group Isomorphism Problem, and Galois theoretic problems.

Some see the beauty of Group Theory in how fundamental it is to so many different areas of mathematics and science.

Conclusion

Finite group theorists focus on two types of problems:

1. *Classification* type problems (e.g. the CFSG); and
2. *Asymptotic* type problems (e.g. counting subgroups of finite groups; asking what a random finite group looks like).

Although the first of these is *a priori* harder, classification problems can be restrictive, and don't always lead to progress in the asymptotic problems that are needed for work on things like the Group Isomorphism Problem, and Galois theoretic problems.

Some see the beauty of Group Theory in how fundamental it is to so many different areas of mathematics and science.

In my view, another huge aspect of its beauty is how quickly one can get from the definition of a group, to deep and important problems.

Conclusion

Finite group theorists focus on two types of problems:

1. *Classification* type problems (e.g. the CFSG); and
2. *Asymptotic* type problems (e.g. counting subgroups of finite groups; asking what a random finite group looks like).

Although the first of these is *a priori* harder, classification problems can be restrictive, and don't always lead to progress in the asymptotic problems that are needed for work on things like the Group Isomorphism Problem, and Galois theoretic problems.

Some see the beauty of Group Theory in how fundamental it is to so many different areas of mathematics and science.

In my view, another huge aspect of its beauty is how quickly one can get from the definition of a group, to deep and important problems.

For example, if you can prove that a 2-generated group G in which $g^5 = 1_G$ for all $g \in G$, is finite, then you will (without a doubt) win a Fields medal...