Enumerating orbits of groups

Lecture 1: Counting orbits and conjugacy classes

Tobias Rossmann

ICTS, Bengaluru — December 2024

Ollscoil na Gaillimhe
University of Galway

Taighde Éireann
Research Ireland

Introduction

These lectures are meant as an introduction to and overview of recent (2016–today) work on generating functions enumerating *linear orbits* and *conjugacy classes* of *unipotent* groups.

- Lecture 1: Counting orbits and conjugacy classes
    - Review of basic facts on group actions
    - Zeta functions enumerating orbits and their relatives
    - Linearising orbit-counting
- Lecture 2: Ask zeta functions
    - Tools for studying ask zeta functions
    - Fundamental properties
    - Key examples
- Tutorial
    - Introduction to the Zeta package for SageMath
    - Baer groups and graphical groups
    - Low nilpotency class suffices
- Lecture 3: A web of themes and open problems
    - Tame vs wild behaviour
    - Rigidity and operations
    - Open problems

Slides and references

These slides and a list of references are available here:
https://torossmann.github.io/cmea

Group actions

Definition

Let G be a group. Let X be a set. A **(right) action** of G on X is a map

$$X \times G \to X, \quad (x, g) \mapsto x.g$$

such that $x.1 = x$ and $(x.g).h = x.(gh)$ for all $x \in X$ and $g, h \in G$.

Example

Each group G acts on itself by **conjugation** $x.g := x^g := g^{-1}xg$.

From now on, we'll usually drop the dot and just write xg.

Orbits

Definition

Given an action of G on X and $x \in X$, the **orbit** of x under G is $xG := \{xg : g \in G\}$.

Fact

The orbits of G on X partition X.

- We write
$$X/G := \{xG : x \in X\}$$
for the **quotient** of X by the action of G.
- The orbits of G acting on itself by conjugation are the **conjugacy classes** of G.
- We write $k(G)$ for the number of conjugacy classes ("**class number**") of G.

The orbit-stabiliser theorem

Definition

Let G act on X. The **stabiliser** of $x \in X$ in G is the subgroup

$$\mathrm{Stab}_G(x) := \{g \in G : xg = x\}.$$

Proposition ("Orbit-stabiliser theorem")

The rule $g \mapsto xg$ *induces a bijection* $\mathrm{Stab}_G(x) \setminus G \to xG$.
In particular, if G *and* X *are finite, then*

$$|xG| = |G : \mathrm{Stab}_G(x)| = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Around the orbit-counting lemma

- Let G be a finite group acting on a finite set X.
- We will now recall two classical formulae for the number of orbits $|X/G|$ of G on X.

Lemma

$|X/G| = \frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}_G(x)|$.

Proof.

By the orbit-stabiliser theorem, we have

$$|X/G| = \sum_{x\in X}|xG|^{-1} = \sum_{x\in X}|G:\mathrm{Stab}_G(x)|^{-1} = \frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}_G(x)|.$$

♦

Around the orbit-counting lemma

The following is often attributed to Burnside, Cauchy, Frobenius, or some combination of these names. For G acting on X as before and $g \in G$, let

$$\mathrm{Fix}(g \mid X) = \left\{x \in X : xg = x\right\}.$$

Lemma ("Orbit-counting lemma")

$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g \mid X)| =$ *average number of fixed points of elements of* G *on* X.

Proof.

- Let $\Sigma = \{(x, g) \in X \times G : xg = x\}$ and note that $|\Sigma| = \sum_{x \in X} |\mathrm{Stab}_G(x)|$.
- By the preceding lemma, we thus have $|\Sigma| = |G| \cdot |X/G|$.
- On the other hand, we also have $|\Sigma| = \sum_{g \in G} |\mathrm{Fix}(g \mid X)|$. ♦

Enumerating orbits

These lectures revolve around the following:

Question

What can we say about $|X/G|$, the number of orbits of G on X?

- Under reasonable hypotheses, for a specific group G acting on a given finite set X, this can often be viewed as belonging to the field of Computational Group Theory.

  That is, $|X/G|$ is a finite number and there are algorithms for finding it.

- In particular, we can try to use software such as GAP or Magma to enumerate orbits.

- This doesn't mean that counting orbits is easy, but at least it's a *single* instance of a *finite* problem.

Enumerating orbits

We'll instead focus on *infinitely* many instances of finite counting problems.

Question

Let $(G_i)_{i \in I}$ be a family of groups, each endowed with an action on a finite set X_i.
Can we determine $|X_i/G_i|$ as a function of the parameter i?
How do these orbit counts depend on i?
What about growth rates or other asymptotic properties of $|X_i/G_i|$?

We'll be particularly interested in the following special case:

Question

Let $(G_i)_{i \in I}$ be a family of finite groups.
What can we say about $k(G_i)$ as a function of i?

Linear orbits

- Unless otherwise indicated, *all rings will be commutative with* 1.
- For a ring R, the group $\mathrm{GL}_d(R)$ (and each of its subgroups) naturally acts on R^d.
- Basic linear algebra describes the linear orbits of $\mathrm{GL}_d(F)$ for a field F. Indeed, if $d \geqslant 1$, then $|F^d/\,\mathrm{GL}_d(F)| = 2$. Over more general rings, the situation is different:

Exercise

Let p be a prime and $d \geqslant 1$. Let $R = \mathbf{Z}/p^n\mathbf{Z}$. Then $|R^d/\,\mathrm{GL}_d(R)| = n + 1$.

Conjugacy classes of general linear groups are more interesting, even over (finite) fields.

Fact

For fixed d*, the number* $k(\mathrm{GL}_d(\mathbf{F}_q))$ *is a polynomial in* q*.*

(This is Exercise 1.190 in Stanley's "Enumerative combinatorics (Vol. 1)".)

Unipotent groups

For a ring R, let

$$U_d(R) = \begin{bmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{bmatrix} \leqslant GL_d(R).$$

By a **unipotent** group, we mean a subgroup of $U_d(R)$ for some d. Linear orbits of $U_d(\mathbf{F}_q)$ can be easily determined.

Exercise

$|\mathbf{F}_q^d / U_d(\mathbf{F}_q)| = dq - d + 1 = d(q-1) + 1$.

Conjecture (Higman 1960)

$k(U_d(\mathbf{F}_q))$ is a polynomial in q.

Exercise

$k(U_3(\mathbf{F}_q)) = q^2 + q - 1$.

Manufacturing unipotent groups

The groups that we'll consider will be unipotent groups of the form

$$\mathbf{G}(R),$$

where we think of $\mathbf{G}$ as a "blueprint" of actual groups obtained by providing rings R such as $\mathbf{Z}/p^n\mathbf{Z}$ (p prime). Important example to keep in mind: $\mathbf{G} = U_d$.

Over the course of these lectures, we'll consider (unipotent) groups constructed out of the following raw materials:

- Graphs ("Graphical groups").
- Alternating bilinear maps ("Baer groups").
- General bilinear maps.
- Nilpotent Lie algebras ("Lazard correspondence").

The last of these group factories is, in a sense, the most general. In particular, for our purposes, *it generates all unipotent groups,* at least when $p \gg 0$.

The Lazard correspondence

- Let p be a prime. The **Lazard correspondence** is an explicit equivalence of categories between
  - finitely generated nilpotent pro-p groups of class $< p$ and
  - finitely generated nilpotent Lie $\mathbf{Z}_p$-algebras of class $< p$.
- This correspondence induces an equivalence between
  - finite p-groups of class $< p$ and
  - finite Lie $\mathbf{Z}_p$-algebras of class $< p$.
- The Lazard correspondence is well-behaved, e.g. with respect to the subgroup and subalgebra structure.

The Lazard correspondence: intrinsic form

- Recall the **Hausdorff series**

$$\begin{aligned} H(X,Y) &= \log(\exp(X)\exp(Y)) \\ &= X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}([X,[X,Y]] + [Y,[Y,X]]) + \cdots \in \mathbf{Q}\langle\langle X, Y\rangle\rangle, \end{aligned}$$

  where X and Y are non-commuting variables. (This needs some work!)
- Given a finitely generated nilpotent Lie $\mathbf{Z}_p$-algebra $\mathfrak{g}$ of class $< p$, we obtain a group $\exp(L)$ with underlying topological space $\mathfrak{g}$ and multiplication $xy = H(x, y)$.

The Lazard correspondence: linear case

- For a ring R, let

$$\mathfrak{n}_d(R) = \begin{bmatrix} 0 & * & \dots & * \\ & 0 & \ddots & \vdots \\ & & \ddots & * \\ & & & 0 \end{bmatrix},$$

  a subalgebra of $\mathfrak{gl}_d(R)$. Note that $a^d = 0$ (associative power!) for all $a \in \mathfrak{n}_d(R)$.

- Suppose that $p \geqslant d$.

  Then the exponential series yields a polynomial bijection

$$\mathfrak{n}_d(\mathbf{Z}_p) \to U_d(\mathbf{Z}_p), \quad a \mapsto \exp(a) = 1 + a + \frac{1}{2}a^2 + \cdots + \frac{1}{(d-1)!}a^{d-1}$$

  with polynomial inverse

$$U_d(\mathbf{Z}_p) \to \mathfrak{n}_d(\mathbf{Z}_p), \quad g \mapsto \log(g) = (g-1) - \frac{1}{2}(g-1)^2 \pm \cdots + \frac{(-1)^d}{d-1}(g-1)^{d-1}.$$

Orbit and class-counting zeta functions v1.0

Let $G \leqslant \mathrm{GL}_d(\mathbf{Z}_p)$ be a (closed) subgroup. For $n \geqslant 0$, let G_n be the (finite!) image of G under the natural map $\mathrm{GL}_d(\mathbf{Z}_p) \twoheadrightarrow \mathrm{GL}_d(\mathbf{Z}/p^n\mathbf{Z})$.

Definition

- The (algebraic) **orbit-counting zeta function** of G is

$$Z_G^{\mathsf{oc}}(T) = \sum_{n=0}^{\infty} |(\mathbf{Z}/p^n\mathbf{Z})^d/G_n| T^n.$$

- The (algebraic) **class-counting zeta function** of G is

$$Z_G^{\mathsf{cc}}(T) = \sum_{n=0}^{\infty} k(G_n) T^n.$$

If you prefer honest "zeta functions" / Dirichlet series: replace T by p^{-s}.

Orbit and class-counting zeta functions v1.0

Some shout-outs:

Remark

- Class-counting zeta functions were introduced by du Sautoy (2005).
- Orbit-counting zeta functions were defined in (R. 2018). They generalise the *similarity class zeta functions* of Avni, Klopsch, Onn, and Voll (2016).
- Berman, Derakhshan, Onn, and Paajanen (2013) studied class-counting zeta functions attached to Chevalley groups.
- Lins (2019, 2020) studied bivariate versions of class-counting zeta functions, enumerating conjugacy classes according to their sizes.

Theorem

- (du Sautoy 2005) $\mathsf{Z}^{\mathrm{cc}}_{\mathrm{G}}(\mathrm{T}) \in \mathbf{Q}(\mathrm{T})$.
- (R. 2018) $\mathsf{Z}^{\mathrm{oc}}_{\mathrm{G}}(\mathrm{T}) \in \mathbf{Q}(\mathrm{T})$.

Without further assumptions on $\mathrm{G} \leqslant \mathrm{GL}_{\mathrm{d}}(\mathbf{Z}_{\mathrm{p}})$, little more seems to be known about these functions!

Module representations

Let R be a ring.

Definition

A **module representation** over R is a module homomorphism $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$, where M, V, and W are R-modules.

A module representation θ gives rise to (and is in fact equivalently determined by) the associated bilinear product

$$*_\theta \colon V \times M \to W$$

defined by $x *_\theta a = x(a\theta)$ ($x \in V$, $a \in M$).

Example

We identify $\mathrm{Hom}(R^d, R^e) = M_{d \times e}(R)$: matrices act by right multiplication on rows. The identity map $M_{d \times e}(R) \to M_{d \times e}(R) = \mathrm{Hom}(R^d, R^e)$ corresponds to the usual product $R^d \times M_{d \times e}(R) \to R^e$.

Module representations

Example

If $M \subset \mathrm{Hom}(V, W)$ is a submodule, then the inclusion $M \hookrightarrow \mathrm{Hom}(V, W)$ is a module representation, which we just call M.

Example

Let $\mathfrak{g}$ be a Lie R-algebra. Then the adjoint representation

$$\mathfrak{g} \to \mathrm{Hom}_{\mathrm{R\text{-}Mod}}(\mathfrak{g}, \mathfrak{g}), \quad a \mapsto [\cdot, a]$$

is a module representation.

Module representations

Example

Let $A(X) = A(X_1, \dots, X_\ell) \in \mathrm{M}_{d\times e}(R[X])$ be a matrix of linear forms. Then $A(X)$ defines a module representation by specialisation

$$R^\ell \to \mathrm{M}_{d\times e}(R), \quad x \mapsto A(x).$$

Conversely, every module representation $R^\ell \to \mathrm{M}_{d\times e}(R)$ is of this form for a unique matrix of linear forms.

Definition

Two module representations $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ and $M' \xrightarrow{\theta'} \mathrm{Hom}(V', W')$ are **isotopic** if a choice of isomorphisms $M \approx M'$, $V \approx V'$, and $W \approx W'$ transforms θ into θ'.

Our terminology goes back to work of Albert (1942). Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation which is **finite free** in the sense that each of M, V, and W is free of finite rank as an R-module. Then θ is isotopic to the module representation associated with a matrix of linear forms.

Average sizes of kernels

Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation involving finite modules (as sets!).

Definition

The average size of the kernel of the elements of M acting as maps $V \to W$ via θ is

$$\mathsf{ask}(\theta) = \frac{1}{|M|} \sum_{a \in M} |\mathrm{Ker}(a\theta)|.$$

For a $\mathbf{Z}_p$-module M, let $M_n = M \otimes_{\mathbf{Z}_p} \mathbf{Z}/p^n\mathbf{Z}$, the "reduction modulo p^n" of M.

Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a finite free module representation over $\mathbf{Z}_p$. We obtain an induced module representation $M_n \xrightarrow{\theta_n} \mathrm{Hom}(V_n, W_n)$ for each $n \geqslant 0$.

Example

Let θ be the module representation $\mathbf{Z}_p^\ell \to \mathrm{M}_{d\times e}(\mathbf{Z}_p)$ associated with a matrix of linear forms $A(X)$. Then θ_n corresponds to simply reducing $A(X)$ modulo p^n.

Ask zeta functions v1.0

Definition

Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a finite free module representation over $\mathbf{Z}_p$. The (algebraic) **ask zeta function** of θ is

$$\mathsf{Z}_\theta^{\mathsf{ask}}(T) = \sum_{n=0}^{\infty} \mathsf{ask}(\theta_n) T^n.$$

Theorem (R. 2018)

$\mathsf{Z}_\theta^{\mathsf{ask}}(T) \in \mathbf{Q}(T)$.

Ask zeta functions generalise and linearise orbit-counting and class-counting zeta functions of unipotent groups as follows.

Ask zeta functions generalise orbit-counting zeta functions

Proposition (R. 2018)

Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}_p)$ *be a Lie subalgebra. Suppose that* $p \geqslant d$. *Let* $G = \exp(\mathfrak{g}) \leqslant U_d(\mathbf{Z}_p)$. *Then* $Z^{\mathsf{oc}}_G(T) = Z^{\mathsf{ask}}_{\mathfrak{g}}(T)$.

Sketch of proof.

- The Lazard correspondence interacts nicely with reduction modulo p^k. We may thus assume that $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}/p^n\mathbf{Z})$ and $G = \exp(\mathfrak{g}) \leqslant U_d(\mathbf{Z}/p^n\mathbf{Z})$. Let $V = (\mathbf{Z}/p^n\mathbf{Z})^d$.
- Our goal is to show that $|V/G| = \mathsf{ask}(\mathfrak{g})$.
- Orbit-counting lemma:

$$|V/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g \mid V)|.$$

- Exercise: $\mathrm{Fix}(\exp(a) \mid V) = \mathrm{Ker}(a \mid V)$.

  Intuition: $\exp(a) \approx 1 + a$ so $x \exp(a) = x$ iff $xa \approx 0$.

♦

Ask zeta functions generalise class-counting zeta functions

Exercise

Let U be a $\mathbf{Z}_p$-submodule of $\mathbf{Z}_p^d$. Then the following are equivalent:

- $\mathbf{Z}_p^d/U$ is torsion-free.
- U is a direct summand of $\mathbf{Z}_p^d$.

We call U **isolated** (as a submodule of $\mathbf{Z}_p^d$) if either condition is satisfied.

Proposition (R. 2018)

Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}_p)$ *be an isolated Lie subalgebra. Let* $p \geqslant d$ *and* $G = \exp(\mathfrak{g}) \leqslant U_d(\mathbf{Z}_p)$*. Then* $Z_G^{cc}(T) = Z_{ad_{\mathfrak{g}}}^{ask}(T)$.

Ask zeta functions generalise class-counting zeta functions

Sketch of proof.

- As in the previous proof, this reduces to the finite case.
- Our goal is to show that $k(G) = \mathsf{ask}(\mathrm{ad}_{\mathfrak{g}})$.
- The class number of G is the average order of a centraliser:

$$k(G) = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|.$$

- Exercise: $C_G(\exp(a)) = \exp(\mathfrak{c}_{\mathfrak{g}}(a))$.
- The claim follows since $\mathfrak{c}_{\mathfrak{g}}(a) = \mathrm{Ker}(\mathrm{ad}_{\mathfrak{g}}(a))$. ♦

Where do we go from here?

- We saw that, excluding small primes, orbit- and class-counting zeta functions of unipotent groups are instances of ask zeta functions.
- A "local version" of this also works for principal congruence subgroups of $\mathfrak{p}$-adic analytic groups.
- Conversely, we'll later see that ask zeta functions always enumerate orbits of suitable groups. (Some of them also enumerate conjugacy classes.)
- Hence, again ignoring small primes, studying ask zeta functions is essentially the same as studying orbit-counting zeta functions of unipotent groups.
- For this translation to be of any value, we need to be able to actually do meaningful things with ask zeta functions!

Compiled on 2024-12-03 at 09:24:49 UTC.