Enumerating orbits of groups

Tutorial

Tobias Rossmann

ICTS, Bengaluru — December 2024

Ollscoil na Gaillimhe
University of Galway

Taighde Éireann
Research Ireland

Topics of this tutorial

- A global perspective on class- and orbit-counting zeta functions.
- Groups from graphs: graphical groups.
- Ask zeta functions $\simeq$ orbit-counting zeta functions of unipotent groups.
- Orbit-counting zeta functions of unipotent groups already arise from commutative groups.
- Class-counting zeta functions of unipotent groups already arise from groups of class 2.

We'll use the first two topics in the third lecture.

We'll cover however much of the greyed out topics time permits.

Globalisation: group functors and group schemes

- A **group functor** is a functor $\mathbf{G}$ from (commutative) rings to groups.

  This just means that $\mathbf{G}$ assigns a group $\mathbf{G}(R)$ to each ring R and a group homomorphism $\mathbf{G}(R) \xrightarrow{\mathbf{G}(\phi)} \mathbf{G}(R')$ to each each ring homomorphism $R \xrightarrow{\phi} R'$ such that identities and composition of homomorphisms are preserved.

- Informally, a *group scheme* is a group functor of geometric origin, defined by the vanishing of polynomial equations, with group operations defined by polynomials.

Example

GL_d (invertible $d \times d$ matrices), SL_d (determinant $= 1$), U_d (unitriangular matrices).

- A *unipotent group scheme* $\mathbf{G}$ yields groups $\mathbf{G}(R) \leqslant \mathrm{U}_d(R)$ (for fixed d) and is defined by the vanishing of polynomial equations. Example: $\mathbf{G} = \begin{bmatrix} 1 & * & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{bmatrix} \leqslant \mathrm{U}_4\,.$
- We can also consider group schemes over a base ring A: instead of arbitrary rings, we consider (commutative, associative, unital) A-algebras R only.
- We'll also assume a *finiteness condition*: $|\mathbf{G}(R)| < \infty$ whenever $|R| < \infty$.

Orbit and class-counting zeta functions v2.0

We obtain better-behaved zeta functions by changing our setting to group schemes.

Definition

Let $\mathbf{G} \leqslant \mathrm{GL}_d \otimes R$ be a group scheme over a ring R.

(Here, $\mathrm{GL}_d \otimes R$ is the group scheme over R obtained from GL_d by base change.)

- The **orbit-counting zeta function** of $\mathbf{G}$ over R is

$$\zeta^{\mathrm{oc}}_{\mathbf{G}}(s) = \sum_{I} |(R/I)^d / \mathbf{G}(R/I)| \cdot |R/I|^{-s}.$$

- The **class-counting zeta function** of $\mathbf{G}$ over R is

$$\zeta^{\mathrm{cc}}_{\mathbf{G}}(s) = \sum_{I} k(\mathbf{G}(R/I)) \cdot |R/I|^{-s}.$$

In each case, the sum is over the ideals I of R with $|R/I| < \infty$.

For our purposes, these definitions generalise our previous ones (sketch on next slide!).

Orbit and class-counting zeta functions v2.0

Sketch:

- Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}_p)$ be an isolated subalgebra. Suppose that $p \geqslant d$. We obtain a group scheme $\mathbf{G} \leqslant \mathrm{U}_d \otimes \mathbf{Z}_p$ over $\mathbf{Z}_p$ via $\mathbf{G}(R) = \exp(\mathfrak{g} \otimes_{\mathbf{Z}_p} R)$.
- We then have $\mathbf{G}(\mathbf{Z}_p) = \exp(\mathfrak{g}) =: G$ and $\mathbf{G}(\mathbf{Z}/p^n\mathbf{Z})$ is the reduction G_n of G modulo p^n (within $\mathrm{GL}_d(\mathbf{Z}_p)$) from before.
- We thus find that

$$\zeta^{\mathsf{oc}}_{\mathbf{G}}(s) = \mathsf{Z}^{\mathsf{oc}}_{G}(p^{-s})$$

and

$$\zeta^{\mathsf{cc}}_{\mathbf{G}}(s) = \mathsf{Z}^{\mathsf{cc}}_{G}(p^{-s}).$$

Orbit and class-counting zeta functions v2.0

The schematic perspective gives rise to well-behaved zeta functions.

For example, the Chinese remainder theorem yields the following Euler products.

Lemma

For a group scheme $\mathbf{G} \leqslant \mathrm{GL}_{\mathrm{d}}$, *we have*

$$\zeta^{\mathsf{oc}}_{\mathbf{G}}(s) = \prod_{p \text{ prime}} \zeta^{\mathsf{oc}}_{\mathbf{G} \otimes \mathbf{Z}_p}(s)$$

and

$$\zeta^{\mathsf{cc}}_{\mathbf{G}}(s) = \prod_{p \text{ prime}} \zeta^{\mathsf{cc}}_{\mathbf{G} \otimes \mathbf{Z}_p}(s).$$

Where can we find interesting but manageable examples of unipotent group schemes?

Baer groups

- Let p be an odd prime. Let A and B be $\mathbf{Z}_p$-modules and let $\#\colon A \times A \to B$ be an alternating bilinear map (i.e. $a\#a = 0$ for all $a \in A$).
- Let $A \xrightarrow{\alpha} \mathrm{Hom}(A, B)$ be the corresponding module representation:

$$a'\alpha = (\cdot)\#a' = a \mapsto a\#a'.$$

- We obtain a group $G_\#$ with underlying set $A \times B$ and multiplication

$$(a, b)(a', b') = \left(a + a', b + b' + \frac{1}{2}a\#a'\right).$$

Exercise

Show that this really defines a group. Moreover, show that

$$[(a, b), (a', b')] = (0, a\#a')$$

for $a, a' \in A$ and $b, b' \in B$.

Class numbers of Baer groups

Lemma

Suppose that $|A|, |B| < \infty$. *Then* $k(G_\#) = |B| \cdot \mathsf{ask}(\alpha)$.

Proof.

We have

$$C_{G_\#}(a', b') = \{(a, b) : a\#a' = 0\} = \mathrm{Ker}(a'\alpha) \times B.$$

and thus

$$k(G_\#) = \frac{1}{|A||B|} \sum_{(a',b')} |\mathrm{Ker}(a'\alpha)| \cdot |B| = |B| \cdot \mathsf{ask}(\alpha). \quad \blacklozenge$$

Baer group schemes

- Let $\#\colon \mathbf{Z}^m \times \mathbf{Z}^m \to \mathbf{Z}^n$ be an alternating bilinear product with associated module representation $\mathbf{Z}^m \xrightarrow{\alpha} M_{m\times n}(\mathbf{Z})$.

- Inspired by the preceding construction, we can construct a group scheme $\mathbf{G}_\#$, the **Baer group scheme** associated with $\#$ such that for each ring R, we may identify $\mathbf{G}_\#(R) = R^m \times R^n$ as sets with commutators satisfying

  $$[(a, b), (a', b')] = (0, a\#a')$$

  for $a, a' \in A$ and $b, b' \in B$.

  (If you're happy to assume that $2 \in R^\times$, you can just use the preceding construction of Baer groups: $\mathbf{G}_\#(R) = G_{\#^R}$. Otherwise, this needs some work.)

- Baer group schemes have class at most 2 (and class precisely 2 unless $\alpha = 0$).

- For finite R, we then obtain $k(\mathbf{G}_\#(R)) = |R|^n \mathsf{ask}(\alpha^R)$ (see the previous lemma).

- Hence, $Z^{\mathsf{cc}}_{\mathbf{G}_\# \otimes \mathbf{Z}_p}(T) = Z^{\mathsf{ask}}_{\alpha^{\mathbf{Z}_p}}(p^n T)$ for each (!) prime p.

Graphical groups

Graphical group (schemes) are particularly friendly examples of Baer groups and Baer group schemes. In particular, we can describe them by means of alternating bilinear products. Here is an equivalent group-theoretic description:

Definition

Let Γ be a (finite, simple) graph with vertices $v_1, \ldots, v_n$. For a ring R, the graphical group $\mathbf{G}_\Gamma(R)$ is defined as follows:

- Generators: $x_1(r), \ldots, x_n(r)$ and $z_{ij}(r)$ for $r \in R$ and $i < j$ with $v_i \sim v_j$.
- Relations:
    - $x_i(r)x_i(r') = x_i(r + r')$ and $z_{ij}(r)z_{ij}(r') = z_{ij}(r + r')$.
    - For $i < j$,
    $$[x_i(r), x_j(r')] = \begin{cases} z_{ij}(rr'), & \text{if } v_i \sim v_j, \\ 1, & \text{otherwise.} \end{cases}$$
    - Each $z_{ij}(r)$ is central.

Graphical groups

Example

We have $\mathbf{G}_{\bullet\!-\!\bullet} \approx U_3$.
Specifically, let

$$X(r) = \begin{bmatrix} 1 & r & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, Y(r) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix}, Z(r) = \begin{bmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We find that $[X(r), Y(s)] = Z(rs)$ and

$$\begin{aligned} U_3(R) = \Big\langle X(r), Y(r), Z(r)\ (r \in R)\ \Big|\ & X(r)X(r') = X(r + r'), \text{etc.}, \\ & [X(r), Y(s)] = Z(rs),\ \text{all } Z(r) \text{ central} \Big\rangle. \end{aligned}$$

Groups from arbitrary module representations

We saw: orbit-counting zeta functions of unipotent groups are ask zeta functions:

Proposition

Let $p \gg 0$, $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}_p)$, *and* $G = \exp(\mathfrak{g}) \leqslant \mathrm{U}_d(\mathbf{Z}_p)$. *Then* $\mathsf{Z}^{\mathsf{oc}}_{G}(s) = \mathsf{Z}^{\mathsf{ask}}_{\mathfrak{g}}(T)$.

We'll now show that conversely, up to a harmless shift, every ask zeta function counts linear orbits. Setup:

- Let $M \xrightarrow{\theta} \mathrm{M}_{d \times e}(\mathbf{Z}_p)$ be a module representation.
- For a $d \times e$ matrix a, let $\hat{a}$ be the invertible $(d+e) \times (d+e)$ matrix

$$\hat{a} = \begin{bmatrix} 1_d & a \\ 0 & 1_e \end{bmatrix}.$$

- Since θ and the induced map $M/\operatorname{Ker}(\theta) \to \mathrm{M}_{d \times e}(\mathbf{Z}_p)$ have the same ask zeta function, we might as well assume that $M \subset \mathrm{M}_{d \times e}(\mathbf{Z}_p)$.

Groups from arbitrary module representations

Proposition

$Z^{\mathsf{oc}}_{\hat{M}}(T) = Z^{\mathsf{ask}}_{M}(p^e T)$.

Proof.

- We show this for each coefficient. Suppose that $M \subset M_{d\times e}(\mathbf{Z}/p^n\mathbf{Z})$.
- Clearly, $(x, y) \in \mathrm{Fix}(\hat{a})$ if and only if $(x, y) = (x, xa + y)$ if and only if $x \in \mathrm{Ker}(a)$. Hence,
$$\mathrm{Fix}(\hat{a}) = \mathrm{Ker}(a) \oplus (\mathbf{Z}/p^n\mathbf{Z})^e.$$
- By the orbit-counting lemma,
$$|(\mathbf{Z}/p^n\mathbf{Z})^{d+e}/\hat{M}| = \frac{1}{|M|}\sum_{a\in M}|\mathrm{Ker}(a)|\cdot p^{ne} = p^{ne}\mathsf{ask}(M). \quad \blacklozenge$$

Groups from arbitrary module representations

Our construction works uniformly for almost all primes $\mathfrak{p}$ as follows:

- Let $M_0 \xrightarrow{\theta} \mathrm{M}_{d\times e}(\mathbf{Z})$ be a module representation.
- Let M be the *isolator* of M_0^θ within $\mathrm{M}_{d\times e}(\mathbf{Z})$. (That is, M/M_0 is the torsion submodule of $\mathrm{M}_{d\times e}(\mathbf{Z})/M_0$.)
- For a ring R, let $RM \subset \mathrm{M}_{d\times e}(R)$ be generated by the image of M.
- Then $\mathsf{Z}^{\mathsf{ask}}_{\theta^{\mathbf{Z}_p}}(T) = \mathsf{Z}^{\mathsf{ask}}_{\mathbf{Z}_p M}(T)$ for $p \gg 0$.
- The rule $R \rightsquigarrow \widehat{RM}$ defines a group scheme $\mathbf{G}_M \leqslant \mathrm{U}_{d+e}$.
- For $p \gg 0$, we have $\mathsf{Z}^{\mathsf{oc}}_{\mathbf{G}_M \otimes \mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{ask}}_{\theta^{\mathbf{Z}_p}}(p^e T)$. Hence, up to finitely many Euler factors, we have $\zeta^{\mathsf{oc}}_{\mathbf{G}_M}(s) \sim \zeta^{\mathsf{ask}}_{\theta}(s-e)$.

Commutative (linear) orbit counts suffice

Proposition

Let $\mathbf{G} \leqslant \mathrm{U}_d$ be a unipotent group scheme. Then there exists a a commutative unipotent group scheme $\mathbf{H} \leqslant \mathrm{U}_{2d}$ such that for $p \gg 0$, we have

$$\mathsf{Z}^{\mathsf{oc}}_{\mathbf{G}\otimes\mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{oc}}_{\mathbf{H}\otimes\mathbf{Z}_p}(p^{-d}T).$$

Sketch of proof.

- Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Q})$ be the Lie algebra of the $\mathbf{Q}$-defined algebraic group associated with $\mathbf{G}$. Let $\mathfrak{g} = \mathfrak{g} \cap \mathfrak{n}_d(\mathbf{Z})$.
- For $p \gg 0$, we have $\mathsf{Z}^{\mathsf{oc}}_{\mathbf{G}\otimes\mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{ask}}_{\mathbf{Z}_p\mathfrak{g}}(T)$.
- Let $\mathbf{H} = \mathbf{G}_{\mathfrak{g}} \leqslant \mathrm{U}_{2d}$. Then $\mathsf{Z}^{\mathsf{oc}}_{\mathbf{H}\otimes\mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{ask}}_{\mathbf{Z}_p\mathfrak{g}}(p^{d}T)$ for $p \gg 0$. ♦

Class-counting zeta functions: reduction to class 2

Proposition (R. & Voll 2024)

Let $\mathbf{G}$ *be a unipotent group scheme of dimension* d *over* $\mathbf{Q}$*. Then there exists a Baer group scheme* $\mathbf{H}$ *dimension* $2d$ *over* $\mathbf{Q}$ *such that for* $p \gg 0$*, we have*

$$\mathsf{Z}^{\mathsf{cc}}_{\mathbf{G}\otimes\mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{cc}}_{\mathbf{H}\otimes\mathbf{Z}_p}(p^{-d}T).$$

In particular, $p^d\, k(\mathbf{G}(\mathbf{F}_p)) = k(\mathbf{H}(\mathbf{F}_p))$ *for* $p \gg 0$*.*

Proof.

- Let $\mathfrak{g}$ be a $\mathbf{Z}$-form of the (rational) Lie algebra of $\mathbf{G}$. Let α be the adjoint representation of $\mathfrak{g}$. The corresponding bilinear product is the Lie bracket $[\cdot,\cdot]$ of $\mathfrak{g}$.
- We know that $\mathsf{Z}^{\mathsf{cc}}_{\mathbf{G}\otimes\mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{ask}}_{\alpha^{\mathbf{Z}_p}}(T)$ for $p \gg 0$.
- Let $\mathbf{H} = \mathbf{G}_{[\cdot,\cdot]}$. Then $\mathsf{Z}^{\mathsf{cc}}_{\mathbf{H}\otimes\mathbf{Z}_p}(T) = \mathsf{Z}^{\mathsf{ask}}_{\alpha^{\mathbf{Z}_p}}(p^dT)$. ♦