Orbits, kernels, and growth of class numbers

Tobias Rossmann

School of Mathematics, Statistics and Applied Mathematics
National University of Ireland, Galway

Lecture notes for talks given at the workshop "*Zeta functions of groups and dynamical systems*" in Düsseldorf, 17–20 September 2018.

1 Introduction

Each group G acts on itself by **conjugation** $g^h := h^{-1}gh$ for $g, h \in G$; the orbits are the **conjugacy classes** of G. For finite G, let $\mathrm{k}(G)$ denote the number of conjugacy classes ("class number") of G. For an explicit formula, by the Orbit-Stabiliser Theorem,

$$\mathrm{k}(G) = \sum_{g\in G} |G : \mathrm{C}_G(g)|^{-1} = \frac{1}{|G|}\sum_{g\in G} |\mathrm{C}_G(g)|$$

is the average size of a centraliser in G. On the other hand, representation theory shows that $\mathrm{k}(G)$ is the number of ordinary irreducible characters of G. The numbers $\mathrm{k}(G)$ have received considerable attention. Of particular interest is "Higman's conjecture":

Conjecture ([7])**.** *For each $d \geqslant 1$, there exists a polynomial $f_d(X)$ such that for each prime power q, $\mathrm{k}(\mathrm{U}_d(\mathbf{F}_q)) = f_d(q)$, where*

$$\mathrm{U}_d = \begin{bmatrix} 1 & * & \dots & \dots & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & * \\ 0 & \dots & \dots & 0 & 1 \end{bmatrix} \leqslant \mathrm{GL}_d\,.$$

These lectures will contribute nothing towards this conjecture. Instead, we will consider zeta functions enumerating linear orbits and conjugacy classes of groups derived primarily from subgroups of $\mathrm{U}_d(\mathbf{Z}_p)$; throughout, p is a prime.

Last modified: 20 September 2018

Reminder: p-adic integers. The ring of **p-adic integers** is the compact local PID

$$\mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z} := \left\{(a_n) \in \prod_{n=0}^{\infty} \mathbf{Z}/p^n\mathbf{Z} : a_{n+1} \equiv a_n \pmod{p^n} \text{ for all } n \geqslant 0\right\}$$

whose unique non-zero prime and unique maximal ideal is $p\mathbf{Z}_p$; we have $\mathbf{Z}_p/p^n\mathbf{Z}_p \approx \mathbf{Z}/p^n\mathbf{Z}$. In the following, little is usually lost by mentally replacing $\mathbf{Z}_p$ by the dense subring

$$\mathbf{Z}_{(p)} := \left\{\frac{a}{b} : a, b \in \mathbf{Z}, p \nmid b\right\} = \mathbf{Z}_p \cap \mathbf{Q};$$

of "rational p-adic integers". The relationship between $\mathbf{Z}_{(p)}$ and $\mathbf{Z}_p$ is similar to that between $\mathbf{Q}$ and $\mathbf{R}$.

Definition. Let $G \leqslant \mathrm{GL}_d(\mathbf{Z}_p)$.

(i) ([6]) The **conjugacy class zeta function** of G is

$$\mathsf{Z}^{\mathsf{cc}}_G(T) = \sum_{n=0}^{\infty} \mathrm{k}(G_n)T^n \in \mathbf{Z}[\![T]\!],$$

where G_n denotes the image of G in $\mathrm{GL}_d(\mathbf{Z}/p^n\mathbf{Z})$.

(ii) ([17]) The **orbit-counting zeta function** of G is

$$\mathsf{Z}^{\mathsf{oc}}_G(T) = \sum_{n=0}^{\infty} |(\mathbf{Z}/p^n\mathbf{Z})^d/G| \cdot T^n \in \mathbf{Z}[\![T]\!].$$

Remark 1.1.

(i) These "zeta functions" become honest Dirichlet series and analytic functions upon replacing T by p^{-s}. In these lectures, we will mostly focus on the local point of view and consider ordinary generating functions as above for fixed p.

(ii) One has to be careful in a global setting in order to e.g. obtain natural Euler products of zeta orbit-counting zeta functions. Namely, if $G \leqslant \mathrm{GL}_d(\mathbf{Z})$, then the function $n \mapsto |(\mathbf{Z}/n\mathbf{Z})^d/G|$ is not usually multiplicative (in the sense of number theory), as already demonstrated by $G = \mathrm{GL}_1(\mathbf{Z}) = \{\pm 1\}$. (The number of orbits of $\{\pm 1\}$ on $\mathbf{Z}/n\mathbf{Z}$ for odd n is $(n+1)/2$.) The same issue arises for class numbers.

Du Sautoy [6] introduced conjugacy class zeta functions and proved their rationality, something we also get for orbit-counting zeta functions.

Theorem 1.2. *(i) (*[6, Thm 1.2]*)* $\mathsf{Z}^{\mathsf{cc}}_G(T) \in \mathbf{Q}(T)$. *(ii) (*[17, Thm 8.3]*)* $\mathsf{Z}^{\mathsf{oc}}_G(T) \in \mathbf{Q}(T)$.

Without further assumptions on G, little more seems to be known about these functions. Berman et al. [3] proved uniformity results with respect to variation of the prime for Chevalley group schemes. Some instances of orbit-counting zeta functions were studied

by Avni et al. [2]. In these lectures, we will see that far more can be said about these functions if we restrict attention to unipotent groups (i.e. subgroups of $\mathrm{U}_d(\mathbf{Z}_p)$).

The study of these zeta functions turns out to borrow heavily from representation growth. However, perhaps surprisingly, orbit-counting zeta functions are often friendlier objects of study. This has to do with powerful forms of duality which have seemingly not been previously encountered in the study of zeta functions of algebraic structures.

Remark 1.3. In most of the following, after minor modifications, $\mathbf{Z}_p$ can be replaced by any compact DVR of characteristic zero (and occasionally even of positive characteristic). This amounts to little more than replacing "p" by either "q" (the residue field size) or "π" (a fixed uniformiser) throughout, depending on context.

2 Average sizes of kernels

Let R be a ring (which we assume to be associative, commutative, and unital).

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

Equivalently (by the "tensor-hom adjunction"), θ is determined by the bilinear map

$$V \times M \to W, \quad (x, a) \mapsto x *_\theta a := x(a\theta).$$

Example 2.1.

(i) The inclusion of a submodule into $\mathrm{Hom}(V, W)$ is a module representation.

(ii) Let $\mathfrak{g}$ be a Lie algebra over R. Then the **adjoint representation** of $\mathfrak{g}$

$$\mathfrak{g} \xrightarrow{\mathrm{ad}_\mathfrak{g}} \mathrm{End}(\mathfrak{g})$$

is the module representation with $*_{\mathrm{ad}_\mathfrak{g}} = [\,\cdot\,,\,\cdot\,]$ (= Lie bracket of $\mathfrak{g}$). Recall that the kernel of $\mathrm{ad}_\mathfrak{g}$ is the centre of $\mathfrak{g}$.

There are numerous useful notions of morphisms between module representations. Inspired by Albert [1], a **homotopy** $\theta \to \tilde{\theta}$ is a triple $(M \xrightarrow{\nu} \tilde{M}, V \xrightarrow{\phi} \tilde{V}, W \xrightarrow{\psi} \tilde{W})$ of module homomorphisms with

$$(x *_\theta a)\psi = (x\phi) *_{\tilde{\theta}} (a\nu)$$

for all $a \in M$ and $x \in V$. An **isotopy** is an invertible homotopy.

Example 2.2.

(i) A Lie algebra homomorphism $\mathfrak{g} \xrightarrow{\phi} \tilde{\mathfrak{g}}$ is a module homomorphism such that (ϕ, ϕ, ϕ) is a homotopy $\mathrm{ad}_\mathfrak{g} \to \mathrm{ad}_{\tilde{\mathfrak{g}}}$. This (faithfully but not fully) embeds the category of Lie R-algebras into the homotopy category of module representations over R.

(ii) Let $A_1, \ldots, A_\ell \in \mathrm{M}_{d\times e}(R)$. Define $A(Z) := Z_1A_1 + \cdots Z_\ell A_\ell$, where the $Z_1, \ldots, Z_\ell$ are algebraically independent indeterminates. We obtain a module representation

$$R^\ell \xrightarrow{A(\,\cdot\,)} \mathrm{M}_{d\times e}(R) = \mathrm{Hom}(R^d, R^e), \quad z \mapsto A(z).$$

Up to isotopy, all module representation involving finitely generated free modules arise in this fashion.

Definition. Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation involving finite modules (as sets!). The **average size of the kernel** of the elements of M acting as linear maps $V \to W$ via θ is

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

Example 2.3. If $\theta = 0$, then $\mathrm{ask}(\theta) = |V|$.

The numbers $\mathrm{ask}(\theta)$ are quite well-behaved with respect to algebraic operations. We will use the following during the tutorial [16] on Zeta [15].

Exercise. Let θ and $\tilde\theta$ be module representations. Let $M\oplus\tilde M \xrightarrow{\theta\oplus\tilde\theta} \mathrm{Hom}(V\oplus\tilde V, W\oplus\tilde W)$ via $(a,\tilde a)(\theta\oplus\tilde\theta) = a\theta \oplus \tilde a\tilde\theta$. Then $\mathrm{ask}(\theta\oplus\tilde\theta) = \mathrm{ask}(\theta)\cdot\mathrm{ask}(\tilde\theta)$ (assuming it makes sense).

The quantities $\mathrm{ask}(\theta)$ enumerate linear orbits of groups:

Lemma 2.4. *Let $|M|, |V|, |W| < \infty$. Define a (linear) action of $(M, +)$ on $V \oplus W$ via*

$$(x, y).a = (x, x(a\theta) + y) \qquad\qquad (x \in V, y \in W).$$

Then $|(V \oplus W)/M| = |W| \cdot \mathrm{ask}(\theta)$.

Proof. $\mathrm{Fix}_{V\oplus W}(a) = \mathrm{Ker}(a\theta) \oplus W$. Orbit-counting lemma: $|X/G| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_X(g)|$. ♦

Less elementarily, numbers of orbits are occasionally precisely the average sizes of kernels associated with module representations. Our key tool is the Lazard correspondence.

Interlude: the Lazard correspondence [11]. Let p be a prime. There is an equivalence of categories between (the evident categories of)

(i) finitely generated nilpotent pro-p groups of class $< p$ and

(ii) finitely generated nilpotent Lie $\mathbf{Z}_p$-algebras of class $< p$.

Recall the **Hausdorff series** (see e.g. [5, Ch. II, §6])

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

where X and Y are non-commuting variables and a rigorous account requires some work.

For an explicit form of the Lazard correspondence, given a Lie $\mathbf{Z}_p$-algebra $\mathfrak{g}$ as above, we obtain a group $\exp(\mathfrak{g})$ with underlying topological space $\mathfrak{g}$ and multiplication $xy = H(x, y)$. The Lazard correspondence is well-behaved, e.g. with respect to the subgroup and subalgebra structure.

Proposition 2.5 ([18, Prop. 6.5]; cf. [14, Thm A])**.** *Let $\mathfrak{g}$ be a finite nilpotent Lie $\mathbf{Z}_p$-algebra of class $< p$. Then* $\mathrm{k}(\exp(\mathfrak{g})) = \mathrm{ask}(\mathrm{ad}_\mathfrak{g})$.

Sketch of proof. Let $G = \exp(\mathfrak{g})$. Then, noting that $\mathfrak{c}_\mathfrak{g}(a) = \mathrm{Ker}(\mathrm{ad}_\mathfrak{g}(a))$ and that the Lazard correspondence behaves well with respect to centralisers,

$$\mathrm{k}(G) = \frac{1}{|G|}\sum_{g\in G}|\mathrm{C}_G(g)| = \frac{1}{|\mathfrak{g}|}\sum_{a\in\mathfrak{g}}|\mathfrak{c}_\mathfrak{g}(a)| = \mathrm{ask}(\mathrm{ad}_\mathfrak{g}). \qquad \blacklozenge$$

Let

$$\mathfrak{n}_d = \begin{bmatrix} 0 & * & \dots & \dots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & * \\ 0 & \dots & \dots & \dots & 0 \end{bmatrix} \subset \mathfrak{gl}_d,$$

the "Lie algebra (scheme) of U_d"; note that subalgebras of $\mathfrak{n}_d$ are nilpotent of class $< d$. We may regard the following as a partial converse of Lemma 2.4.

Proposition 2.6 ([17, §8])**.** *Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}/p^n\mathbf{Z})$ be a subalgebra, where $p \geqslant d$. Let $G := \exp(\mathfrak{g}) \leqslant \mathrm{U}_d(\mathbf{Z}/p^n\mathbf{Z})$. Then* $|(\mathbf{Z}/p^n\mathbf{Z})^d/G| = \mathrm{ask}(\mathfrak{g})$.

Remark 2.7.

(i) For $p \geqslant d$, every subgroup of $\mathrm{U}_d(\mathbf{Z}_p)$ is of the form $\exp(\mathfrak{g})$ for a subalgebra $\mathfrak{n}_d(\mathbf{Z}_p)$.

(ii) The nilpotence assumptions can be dropped at the cost of having to replace $\exp(\mathfrak{g})$ by a suitable "congruence subgroup"; see [17, §8] and Proposition 5.3 below.

Sketch of proof of Proposition 2.6. Write $V = (\mathbf{Z}/p^n\mathbf{Z})^d$. Then

$$|V/G| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_V(g)| = \frac{1}{|\mathfrak{g}|}\sum_{a\in\mathfrak{g}}|\mathrm{Ker}(a)| = \mathrm{ask}(\mathfrak{g}). \qquad \blacklozenge$$

Summary. For fixed nilpotency class and after discarding small primes, the numbers of orbits of unipotent p-groups and the quantities $\mathrm{ask}(\theta)$ essentially coincide and class numbers are among the latter numbers. This correspondence is valuable since, as we will now see, the numbers $\mathrm{ask}(\theta)$ can be studied using a variety of techniques—some of these may seem quite unrelated to our group-theoretic points of departure.

Proposition 5.6 can be used to deduce Lins's formula [13] for the conjugacy class zeta function of the free nilpotent pro-p group $F_{2,d}$ of class 2 on d generators; see [18, Ex. 7.3]. Indeed, the associated Lie $\mathbf{Z}_p$-algebra is $\mathfrak{f}_{2,d} = V \oplus (V \wedge V)$ with commutation induced by $\wedge$ and $V = \mathbf{Z}_p^d$. The adjoint representation of $\mathfrak{f}_{2,d}$ is the direct sum of λ from the preceding proof and $V \wedge V \xrightarrow{0} \mathrm{Hom}(V \wedge V, V)$. Using the natural notion of conjugacy class zeta functions for group schemes (see [18]), for $p \neq 2$, it follows that

$$\mathsf{Z}^{\mathsf{cc}}_{F_{2,d}}(T) = \mathsf{Z}^{\mathsf{ask}}_{\mathfrak{so}_d(\mathbf{Z}_p)}\left(p^{\binom{d}{2}}T\right).$$

Further explicit examples of ask and conjugacy class zeta functions will be discussed as part of the tutorial on Zeta [16].

6 Open problems

A common problem in the theory of local zeta functions (such as $\zeta_\theta(s) := \mathsf{Z}_\theta(p^{-s})$ for a module representation θ over $\mathbf{Z}_p$) is to interpret (the real parts of the meromorphic continuations of) their poles. In the case of Igusa's local zeta function, such an interpretation is proposed by the famous (and still open) Monodromy Conjecture [8]. Nothing akin to the Monodromy Conjecture seems to have been formulated for any of the types of local zeta functions studied in asymptotic algebra, including ask zeta functions.

I would like to finish by asking a more humble question.

Question. *What can we say about the smallest real pole, ω_θ say, of $\zeta_\theta(s)$?*

The *largest* real pole α_θ of $\zeta_\theta(s)$ is precisely the abscissa of convergence of $\zeta_\theta(s)$. As is well known, it coincides with the degree of polynomial growth of the partial sums of the coefficients of $\mathsf{Z}_\theta(T)$. It is easy to produce elementary (and in some sense optimal) general estimates for α_θ; see [17, Prop. 3.3]. The study of ω_θ, on the other hand, seems to have a very different flavour.

Problem. *Characterise those θ with $\omega_\theta \geqslant 0$ (resp. $\omega_\theta > 0$).*

The non-negativity of ω_θ is related to $\mathsf{Z}_\theta(T)$ "almost" having integral coefficients (see the Zeta tutorial). The latter condition generalises the relationship between ask and orbit-counting zeta functions from above. A more appealing version of the preceding problem thus asks for an answer to the following.

Question. *Suppose that $p^N \mathsf{Z}_\theta(T) \in \mathbf{Z}[\![T]\!]$. What do the coefficients count?*

Experimental evidence suggests that the positivity of ω_θ plays the role of a "generalised unipotence" condition on the (suspected) underlying counting problem.

References

[1] A. A. Albert, *Non-associative algebras. I. Fundamental concepts and isotopy*, Ann. of Math. (2) **43** (1942), 685–707.

[2] N. Avni, B. Klopsch, U. Onn, and C. Voll, *Similarity classes of integral p-adic matrices and representation zeta functions of groups of type A_2*, Proc. Lond. Math. Soc. (3) **112** (2016), no. 2, 267–350. arXiv:1410.4533.

[3] M. N. Berman, J. Derakhshan, U. Onn, and P. Paajanen, *Uniform cell decomposition with applications to Chevalley groups*, J. Lond. Math. Soc. (2) **87** (2013), no. 2, 586–606. arXiv:1106.2885.

[4] A. Boralevi, D. Faenzi, and E. Mezzetti, *Linear spaces of matrices of constant rank and instanton bundles*, Adv. Math. **248** (2013), 895–920.

[5] N. Bourbaki, *Éléments de mathématique. Fasc. XXXVII. Groupes et algèbres de Lie. Chapitres 2 et 3.*, Hermann, Paris, 1972. Actualités Scientifiques et Industrielles, No. 1349.

[6] M. P. F. du Sautoy, *Counting conjugacy classes*, Bull. London Math. Soc. **37** (2005), no. 1, 37–44.

[7] G. Higman, *Enumerating p-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30.

[8] J.-i. Igusa, *b-functions and p-adic integrals*, Algebraic analysis, Vol. I, 1988, pp. 231–241.

[9] ———, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, Providence, RI: American Mathematical Society, 2000.

[10] D. E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.

[11] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190.

[12] N. Linial and D. Weitz, *Random vectors of bounded weight and their linear dependencies (unpublished manuscript)* (2000). `http://www.drorweitz.com/ac/pubs/rand_mat.pdf`.

[13] P. M. Lins de Araujo, *Bivariate representation and conjugacy class zeta functions associated to unipotent group schemes, II: Groups of type F, G, and H (preprint)* (2018). arXiv:1805.02040.

[14] E. A. O'Brien and C. Voll, *Enumerating classes and characters of p-groups*, Trans. Amer. Math. Soc. **367** (2015), no. 11, 7775–7796. arXiv:1203.3050.

[15] T. Rossmann, `Zeta`*, version 0.3.2*, 2017. See `http://www.maths.nuigalway.ie/~rossmann/Zeta/`.

[16] ———, *An introduction to* `Zeta`, 2018. A Sage notebook. See `http://www.maths.nuigalway.ie/~rossmann/files/zetatut.ipynb`.

[17] ———, *The average size of the kernel of a matrix and orbits of linear groups*, Proc. Lond. Math. Soc. (3) **117** (2018), no. 3, 574–616.

[18] ———, *The average size of the kernel of a matrix and orbits of linear groups, II: duality (preprint)* (2018). arXiv:1807.01101.

[19] C. Voll, *Functional equations for zeta functions of groups and rings*, Ann. of Math. (2) **172** (2010), no. 2, 1181–1218. arXiv:math/0612511.