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

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

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

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

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

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 $A(Z) := Z_1 A_1 + \cdots Z_\ell A_\ell$, 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 **<u>a</u>verage <u>s</u>ize of the <u>k</u>ernel** 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,

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

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

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

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.

3 Ask zeta functions

In the same way that we strung together class numbers and numbers of orbits to define conjugacy class and orbit-counting zeta functions, respectively, we now consider zeta functions arising from suitable numbers $\mathrm{ask}(\theta)$.

3.1 Basics

Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation over $\mathbf{Z}_p$. Suppose that M, V, and W are free of finite ranks ℓ, d, and e, respectively. After chosing bases, θ becomes a module representation $\mathbf{Z}_p^\ell \to \mathrm{M}_{d\times e}(\mathbf{Z}_p)$. For $y \in \mathbf{Z}_p$, let θ_y be the induced module representation

$$(\mathbf{Z}_p/y\mathbf{Z}_p)^\ell \to \mathrm{M}_{d\times e}(\mathbf{Z}_p/y\mathbf{Z}_p).$$

Definition ([17, 18])**.** The **ask zeta function** of θ is

$$\mathsf{Z}_\theta^{\mathsf{ask}}(T) := \sum_{n=0}^{\infty} \mathrm{ask}(\theta_{p^n})T^n \in \mathbf{Q}[\![T]\!].$$

We often drop the superscript "ask" in the following. If ι is the inclusion of a submodule M into $\mathrm{M}_{d\times e}(\mathbf{Z}_p)$, then just write $\mathsf{Z}_M(T) := \mathsf{Z}_\iota(T)$.

Example 3.1. By Example 2.3, $\mathsf{Z}_{\{0_{d\times e}\}}(T) = \sum\limits_{n=0}^{\infty} p^{dn}T^n = \frac{1}{1-p^dT}$.

Propositions 2.5–2.6 yield the following.

Theorem 3.2 ([17, Thm 1.7])**.** *Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z}_p)$, where $p \geqslant d$. Write $G = \exp(\mathfrak{g})$.*

(i) $\mathsf{Z}_G^{\mathsf{oc}}(T) = \mathsf{Z}_{\mathfrak{g}}^{\mathsf{ask}}(T)$.

(ii) Suppose that $\mathfrak{g}$ is an **isolated** *submodule of $\mathfrak{n}_d(\mathbf{Z}_p)$—this means that the $\mathbf{Z}_p$-module $\mathfrak{n}_d(\mathbf{Z}_p)/\mathfrak{g}$ is torsion-free and is equivalent to $\mathfrak{g}$ being a direct summand of $\mathfrak{n}_d(\mathbf{Z}_p)$. Then $\mathsf{Z}_G^{\mathsf{cc}}(T) = \mathsf{Z}_{\mathrm{ad}_{\mathfrak{g}}}^{\mathsf{ask}}(T)$.*

Remark 3.3.

(i) If $\mathfrak{g}$ is isolated, then the reduction modulo p^n of $\mathfrak{g}$ within $\mathfrak{gl}_d(\mathbf{Z}_p)$ agrees with the same "internal" operation for $\mathfrak{g}$. More formally, it allows us to identify $\mathfrak{g} \otimes \mathbf{Z}/p^n\mathbf{Z}$ with the image of $\mathfrak{g}$ in $\mathfrak{gl}_d(\mathbf{Z}/p^n\mathbf{Z})$.

(ii) ([17, Rem. 8.18]) Let $\mathfrak{g} = p\mathfrak{n}_2(\mathbf{Z}_p) = \begin{bmatrix} 0 & p\mathbf{Z}_p \\ 0 & 0 \end{bmatrix}$ and $G = \exp(\mathfrak{g}) = \begin{bmatrix} 1 & p\mathbf{Z}_p \\ 0 & 1 \end{bmatrix} \leqslant \mathrm{U}_2(\mathbf{Z}_p)$. The image of G in $\mathrm{U}_2(\mathbf{Z}/p\mathbf{Z})$ is trivial whence

$$\mathsf{Z}_G^{\mathsf{cc}}(T) = 1 + T + \mathcal{O}(T^2).$$

On the other hand, $\mathrm{ad}_{\mathfrak{g}} = 0$ (and $\mathrm{rk}_{\mathbf{Z}_p}(\mathfrak{g}) = 1$) so that

$$\mathsf{Z}_{\mathrm{ad}_{\mathfrak{g}}}(T) = \frac{1}{1-pT} = 1 + pT + \mathcal{O}(T^2)$$

by Example 3.1. This issue is really an artifact of our less than ideal (in this situation) definition of conjugacy class zeta functions; see [18, §6.1].

3.2 p-Adic integration and uniformity

Theorem 3.2 allows us to study instances of conjugacy class and orbit-counting zeta functions in the setting of ask zeta functions. Our next goal, is to have a closer look at the latter. Let $M = \mathbf{Z}^\ell \xrightarrow{\theta} \mathrm{M}_{d\times e}(\mathbf{Z}_p)$ be as before. Define

$$\mathrm{K}_\theta \colon M \times \mathbf{Z}_p \to [0,\infty], \quad (a,y) \mapsto |\mathrm{Ker}(\underbrace{a_y\theta_y}_{=(a\theta)_7})|,$$

Let $|\cdot|_p$ be the usual p-adic absolute value (on $\mathbf{Z}_p$, say) with $|p|_p = p^{-1}$. It is straightforward to express the average in the definition of $\mathrm{ask}(\theta)$ as an integral:

Proposition 3.4 ([17, Thm 4.5])**.** *For $s \in \mathbf{C}$ with $\mathrm{Re}(s) > d$,*

$$(1-p^{-1}) \cdot \mathsf{Z}_\theta(p^{-s}) = \int\limits_{M\times\mathbf{Z}_p} |y|_p^{s-1}\, \mathrm{K}_\theta(a,y)\, \mathrm{d}\mu(a,y), \tag{3.1}$$

where μ denotes the Haar measure on $M \times \mathbf{Z}_p$ with total volume 1.

Recall that, up to isotopy (which does not affect ask zeta functions), we may assume that $a\theta = A(a)$, where $A(Z)$ is a $d \times e$-matrix of linear forms in ℓ variables over $\mathbf{Z}_p$. By mimicking arguments of Voll [19, §2.2], we can express $\mathrm{K}_\theta(a,y)$ in terms of p-adic maximum norms of minors of $A(a)$ and y as follows:

Lemma 3.5 ([17, Cor. 4.9])**.** *Let $f_i(Z)$ be the set of $i \times i$-minors of $A(Z)$. Let $r = \max(\mathrm{rk}_{\mathbf{Q}_p}(A(a)) : a \in M)$ and let $N = \{a \in M : \mathrm{rk}_{\mathbf{Q}_p}(A(a)) < r\}$. Then N has measure zero (w.r.t. the normalised Haar measure on M) and for all $a \in M \setminus N$ and $y \in \mathbf{Z}_p \setminus \{0\}$,*

$$\mathrm{K}_\theta(a,y) = |y|_p^{r-d} \prod_{i=1}^{r} \frac{\|f_{i-1}(a)\|_p}{\|f_i(a) \cup y f_{i-1}(a)\|_p}.$$

Proof. Fix $a \in M \setminus N$ and $y \in \mathbf{Z}_p \setminus \{0\}$. Define n via $|y|_p = p^{-n}$. By basic linear algebra ("elementary divisor theorem", "Smith normal form"), there are integers $0 \leqslant \lambda_1 \leqslant \cdots \leqslant \lambda_r$ and matrices $R \in \mathrm{GL}_d(\mathbf{Z}_p)$ and $S \in \mathrm{GL}_e(\mathbf{Z}_p)$ such that

$$RA(a)S = \mathrm{diag}(p^{\lambda_1}, \dots, p^{\lambda_r}, 0, \dots, 0) =: D.$$

Linear algebra also tells us that $A(a)$ and D have the same ideals of minors of any order. Since the ideal of $i \times i$ minors of D is generated by $p^{\lambda_1+\cdots+\lambda_i}$, we obtain $\|f_i(a)\| = p^{-\lambda_1-\cdots-\lambda_i}$. By inspection of D, it easily follows that

$$\mathrm{K}_\theta(a,y) = p^{\min(\lambda_1,n)+\cdots+\min(\lambda_r,n)+(d-r)n}$$

and the claim follows since

$$p^{\min(\lambda_i,n)} = \frac{1}{\max(p^{-\lambda_i}, p^{-n})} = \frac{p^{-\lambda_1-\cdots-\lambda_{i-1}}}{\max(p^{-\lambda_1-\cdots-\lambda_i}, p^{-n-\lambda_1-\cdots-\lambda_{i-1}})} = \frac{\|f_{i-1}(a)\|}{\|f_i(a) \cup y f_{i-1}(a)\|}. \quad \blacklozenge$$

This provides an explicit ("polynomial") form of (3.1). Deep results from p-adic integration that we will not discuss here (namely, the rationality of Igusa's local zeta function [9, Ch. 8]) now imply the following.

Theorem 3.6 ([17, Thm 4.10])**.** $\mathsf{Z}_\theta(T) \in \mathbf{Q}(T)$. *More precisely, there are* $m \in \mathbf{N}_0$ *and non-zero* $(a_1, b_1), \dots, (a_u, b_u) \in \mathbf{Z} \times \mathbf{N}_0$ *such that* $p^m \prod\limits_{i=1}^{u}(1 - p^{a_i}T^{b_i})\mathsf{Z}_\theta(T) \in \mathbf{Z}[T]$.

Our proof of rationality relies on resolution of singularities and is thus generally impractical. In a suitable "global setting" it is natural to consider the behaviour of ask zeta functions associated with families of module representations indexed by primes. Here, further tools from p-adic integration going back to Denef (see [9]) establish "uniformity" under variation of the prime in the following sense.

Theorem 3.7 ([17, Thm 4.11])**.** *Let* $\mathbf{Z}^\ell \xrightarrow{\theta} \mathrm{M}_{d\times e}(\mathbf{Z})$ *be a module representation. There are* $W_1(X,T), \dots, W_r(X,T) \in \mathbf{Q}(X,T)$ *(which can be written over denominators of the same shape as above) and* $\mathbf{Q}$*-defined varieties* $V_1, \dots, V_r$ *such that for almost all* p*,*

$$\mathsf{Z}_{\theta\otimes\mathbf{Z}_p}(T) = \sum_{i=1}^{r} |\bar{V_i}(\mathbf{F}_p)| \cdot W_i(p,T),$$

where $\bar{\cdot}$ *denotes reduction modulo* p *of fixed* $\mathbf{Z}$*-forms.*

Remark 3.8. The following comments are research problems in disguise:

(i) By combining Theorems 3.2 and 3.7, we obtain similar uniformity results for orbit-counting and conjugacy class zeta functions of groups of $\mathbf{Z}_p$-points of "unipotent group schemes". At the opposite end of the group-theoretic spectrum, Berman et al. [3] proved uniformity for conjugacy class zeta functions associated with Chevalley group schemes. It is not known if orbit-counting and conjugacy class zeta functions associated with general linear group $\mathbf{Z}$-schemes are uniform in the above sense.

(ii) It is unknown how wild the varieties V_i "required" to produce uniform formulae for ask zeta functions as in Theorem 3.7 are. As a lower bound, a positive proportion of $\mathbf{Q}$-defined elliptic curves (suitably ordered by height) arise; see [17, §7]. Despite such subtle arithmetic and geometric issues, as we will soon now see, many natural examples of ask zeta functions can not only be computed (without constructing a resolution of singularities, say) but are actually surprisingly tame, a marked departure from representation and subobject zeta functions.

Remark 3.9 (Global ask zeta functions)**.** Let θ be as in Theorem 3.7. Define the **global ask zeta function** of θ to be the Dirichlet series $\zeta_\theta(s) = \sum\limits_{n=1}^{\infty} \mathrm{ask}(\theta \otimes \mathbf{Z}/n\mathbf{Z})n^{-s}$. Then it is easy to see that (see [17, Prop. 3.4])

(i) $\zeta_\theta(s)$ converges for $\mathrm{Re}(s) > d + 1$ and

(ii) $\zeta_\theta(s) = \prod\limits_{p} \mathsf{Z}_{\theta\otimes\mathbf{Z}_p}(p^{-s})$.

Deeper insight into $\zeta_\theta(s)$ (e.g. the existence of meromorphic continuation) can be gained using Theorem 3.7 and results from subobject and representation growth; see [17, §4.5]. However, as explained in Remark 1.1(ii), such results do not immediately translate to the setting of conjugacy class and orbit-counting zeta functions.

3.3 Constant rank spaces

For a surprising number of interesting examples, the actual shapes of ask zeta functions are far removed from the complexity predicted by Theorem 3.7.

Exercise. Show that $\mathsf{Z}_{\mathrm{M}_1(\mathbf{Z}_p)}(T) = \frac{1-p^{-1}T}{(1-T)^2}$.

More generally, we will later show that

$$\mathsf{Z}_{\mathrm{M}_{d\times e}(\mathbf{Z}_p)}(T) = \frac{1-p^{-e}T}{(1-T)(1-p^{d-e}T)}. \tag{3.2}$$

A naive attempt to prove this would produce a formula for K_θ; this quickly becomes cumbersome. We will see that there is a much better way of thinking about (3.2).

Definition 3.10. Let F be a field. A subspace $M \subset \mathrm{M}_{d\times e}(F)$ has **constant rank** r if $M \neq 0$ and $\mathrm{rk}(a) = r$ for all $a \in M \setminus \{0\}$.

Example 3.11. Let D be a d-dimensional division algebra over F. Then the regular representation of D embeds D as a subspace of $\mathrm{M}_d(F)$ of constant rank d.

Constant rank spaces have been studied extensively in the literature; see e.g. [4]. They constitute a major source of well-behaved ask zeta functions:

Theorem 3.12 (See [17, §6] and [18, §3.6].)**.** *Let $M \subset \mathrm{M}_{d\times e}(\mathbf{Z}_p)$ be an isolated submodule of $\mathbf{Z}_p$-rank ℓ. Let $r = \max(\mathrm{rk}_{\mathbf{Q}_p}(a) : a \in M)$. Suppose that the reduction of M modulo p has constant rank r over $\mathbf{F}_p$. Then*

$$\mathsf{Z}_M(T) = \frac{1-p^{d-r-\ell}T}{(1-p^{d-\ell}T)(1-p^{d-r}T)}.$$

Sketch of proof. Let $\mathrm{M}_{d\times e}(\mathbf{Z}_p) \xrightarrow{\bar{\cdot}} \mathrm{M}_{d\times e}(\mathbf{F}_p)$ denote reduction modulo p. Since M is isolated, $\bar{\cdot}$ induces an isomorphism $M/pM \approx \bar{M}$. Next, one reduces the computation of $\mathrm{K}_M(a,y)$ to the case that $a \in M \setminus pM$. Since $\bar{M}$ has constant rank r, $\mathrm{K}_M(a,p) = p^{d-r}$ and, more generally,

$$\mathrm{K}_M(a,y) = |y|^{r-d} \tag{3.3}$$

for all $y \in \mathbf{Z}_p \setminus \{0\}$. The evaluation of our integral is then straightforward. ♦

Remark 3.13.

(i) If M is not isolated, some element of $M \setminus pM$ vanishes modulo p and (3.3) fails.

(ii) The assumptions of Theorem 3.12 imply that $M \otimes \mathbf{Q}_p$ has constant rank r.

Even though $\mathrm{M}_{d\times e}(\mathbf{Q}_p)$ is far removed from having constant rank, equation (3.2) suggests that there might be a module

$$M^\bullet \subset \mathrm{M}_{d\times \boxed{?}}(\mathbf{Z}_p)$$

of $\mathbf{Z}_p$-rank e and constant rank d modulo p with $\mathsf{Z}_M(T) = \mathsf{Z}_{M^\bullet}(T)$. Our next goal is to define a natural operation $M \mapsto M^\bullet$ which indeed has the desired properties when applied to $\mathrm{M}_{d\times e}(\mathbf{Z}_p)$.

4 Knuth duality

Let R be a ring and $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation. Let $(\,\cdot\,)^* = \mathrm{Hom}(\,\cdot\,, R)$ be the usual dual of R-modules. Recall that for $A \xrightarrow{\alpha} B$, α^* is the map $B^* \to A^*$ given by $\psi\alpha^* = \alpha\psi$. Up to taking duals, we can "permute" the modules M, V, and W to derive further module representations. We only spell out the three "involutions"; recall that $x *_\theta a = x(a\theta)$ for $x \in V$ and $a \in M$.

Definition. The **Knuth duals** of θ are:

(i) $V \xrightarrow{\theta^\circ} \mathrm{Hom}(M, W)$ with $a *_{\theta^\circ} x = x *_\theta a$ for $a \in M$ and $x \in V$.

(ii) $W^* \xrightarrow{\theta^\bullet} \mathrm{Hom}(V, M^*)$ with $a(x *_{\theta^\bullet} \psi) = (x *_\theta a)\psi$ for $a \in M$, $x \in V$, and $\psi \in W^*$.

(iii) $M \xrightarrow{\theta^\vee} \mathrm{Hom}(W^*, V^*)$ with $a\theta^\vee = (a\theta)^*$ for $a \in M$.

Proposition 4.1 ([18, §4, Rem. 5.5]). *If R is a proper quotient of a Dedekind domain, then*

$$\begin{aligned}(1,2) &\mapsto \circ,\\ (1,3) &\mapsto \bullet,\\ (2,3) &\mapsto \vee\end{aligned}$$

defines an action of S_3 on isotopy classes of module representation involving finitely generated modules over R.

Example 4.2. Let $A(Z) \in \mathrm{M}_{d\times e}(R[Z_1, \dots, Z_\ell])$ be a matrix of linear forms. Define c_{hij} by $A(Z) = \left[\sum\limits_{h=1}^{\ell} c_{hij} Z_h\right]_{ij}$. Then, up to isotopy, $\circ$, $\bullet$, and $\vee$ simply permute the indices of c_{hij}. For $\ell = d = e$, this is the setting considered by Knuth [10]; his work is widely used in the theory of "semifields". For instance, it is common to only classify semifields up to "Knuth orbits".

Theorem 4.3 ([18, Thm 5.2]). *Let R be a finite quotient of a Dedekind domain (e.g. $R = \mathbf{Z}/n\mathbf{Z}$, for $n \neq 0$). Then (assuming finiteness of all relevant modules below): (i)* $\mathrm{ask}(\theta^\circ) = \frac{|M|}{|V|}\,\mathrm{ask}(\theta)$*. (ii)* $\mathrm{ask}(\theta^\bullet) = \mathrm{ask}(\theta)$*. (iii)* $\mathrm{ask}(\theta^\vee) = \frac{|W|}{|V|}\,\mathrm{ask}(\theta)$.

Proof.

(i) This part goes back to an unpublished note of Linial and Weitz [12]. Let

$$C(\theta) = \{(x,a) \in V \times M : x *_\theta a = 0\}$$

and note that $(x,a) \in C(\theta)$ if and only if $(a,x) \in C(\theta^\circ)$. Clearly, $\operatorname{ask}(\theta) = \frac{|C(\theta)|}{|M|}$ whence

$$\operatorname{ask}(\theta^\circ) = \frac{|C(\theta^\circ)|}{|V|} = \frac{|C(\theta)|}{|V|} = \frac{|M|}{|V|}\operatorname{ask}(\theta).$$

(iii) Using primary decomposition, one finds that if U is a finitely generated R-module, then U is reflexive and $U \approx U^*$ (non-canonically). Now

$$\begin{aligned} |C(\theta^\vee)| &= |\{(\psi,a) \in W^* \times M : \forall x \in V.(x(a\theta))\psi = 0\}| \\ &= |\{(\psi,a) \in W^* \times M : \operatorname{Im}(a\theta) \subset \operatorname{Ker}(\psi)\}| \\ &= \sum_{a \in M} |(W/\operatorname{Im}(a\theta))^*| = \sum_{a\in M} |W/\operatorname{Im}(a\theta)| = \frac{|W|}{|V|}\sum_{a \in M}|\operatorname{Ker}(a\theta)|. \end{aligned}$$

(ii) Use $\theta^{\circ\vee\circ} = \theta^\bullet$ and combine (i) and (iii). ♦

Corollary 4.4 ([14]). *Let $\mathfrak{g}$ be a finite nilpotent Lie $\mathbf{Z}_p$-algebra of class $< p$. Then*

$$\operatorname{k}(\exp(\mathfrak{g})) = \operatorname{ask}(\operatorname{ad}_{\mathfrak{g}}^\bullet).$$ ♦

Indeed, using the Kirillov orbit method, the right-hand side is seen to enumerate the irreducible characters of $\exp(\mathfrak{g})$; however, as we have seen, the latter method is not required to deduce the preceding corollary.

Corollary 4.5. *Given a module representation $\mathbf{Z}_p^\ell \xrightarrow{\theta} \mathrm{M}_{d\times e}(\mathbf{Z}_p)$,*

$$\mathsf{Z}_\theta(T) = \mathsf{Z}_{\theta^\circ}(p^{d-\ell}T) = \mathsf{Z}_{\theta^\bullet}(T) = \mathsf{Z}_{\theta^\vee}(p^{d-e}T).$$ ♦

This means that there are potentially different ways of computing a single ask zeta functions, e.g. by means of a p-adic integral as in Proposition 3.4.

5 Applications to zeta functions

We now illustrate how Knuth duality can be employed in the calculation of specific examples of ask, orbit-counting, and conjugacy class zeta functions.

Proposition 5.1 ([17, Prop.1.5]).

$$\mathsf{Z}_{\mathrm{M}_{d\times e}(\mathbf{Z}_p)}(T) = \frac{1-p^{-e}T}{(1-T)(1-p^{d-e}T)} = 1 + (1 + p^{d-e} - p^{-e})T + \mathcal{O}(T^2).$$

Proof. One checks that, up to isotopy, the $\bullet$-dual of the identity, ι say, on $\mathrm{M}_{d\times e}(\mathbf{Z}_p)$ is represented by $\mathrm{diag}([Z_1,\dots,Z_e],\dots,[Z_1,\dots,Z_e])$ (d copies). Assuming this, the associated submodule of $\mathrm{M}_{d\times de}(\mathbf{F}_p)$ has constant rank d and the claim follows from Theorem 3.12.

Regarding $\iota^\bullet$, write $V = \mathbf{Z}_p^d$ and $W = \mathbf{Z}_p^e$. Then $\iota^\bullet$ is a module representation

$$W^* \to \mathrm{Hom}(V, \mathrm{Hom}(V,W)^*).$$

Now $\mathrm{Hom}(V,W) \approx V^* \otimes W$ and thus $\mathrm{Hom}(V,W)^* \approx V^{**} \otimes W^* \approx W^* \otimes V$ (all naturally). It follows easily that we may identify $\iota^\bullet$ and the module representation

$$W^* \xrightarrow{\theta} \mathrm{Hom}(V, W^* \otimes V),$$

with $x *_\theta \psi = \psi \otimes x$ ($x \in V$, $\psi \in W^*$). The matrix of linear forms from above is obtained by choosing the evident bases. ♦

Remark 5.2. From our point of view, Linial and Weitz [12] used $\circ$-duality to compute the coefficient of T of $\mathsf{Z}_{\mathrm{M}_{d\times e}(\mathbf{Z}_p)}(T)$. Using the above integral formalism, their arguments easily yields another proof of Proposition 5.1 (which is exactly the proof given in [17]). While the latter proof is slightly easier, taking the $\bullet$-dual as we did makes the connection with constant rank spaces more explicit.

We now discuss some genuinely group-theoretic applications. As previously indicated, our arguments for unipotent groups can be adapted to the general case by passing to congruence subgroups.

Proposition 5.3 ([17, §8.4])**.** *Let $p \neq 2$ and let $\mathfrak{g} \subset \mathfrak{gl}_d(\mathbf{Z}_p)$ be a Lie subalgebra. Let $G = \exp(p\mathfrak{g}) \leqslant \mathrm{GL}_d^1(\mathbf{Z}_p)$. Then $\mathsf{Z}_G^{\mathsf{oc}}(T) = 1 + p^d T \cdot \mathsf{Z}_{\mathfrak{g}}^{\mathsf{ask}}(T)$.*

Remark 5.4. More generally, suppose that $m > 1/(p-1)$. Let $G^m = \exp(p^m\mathfrak{g})$. Then

$$\mathsf{Z}_{G^m}^{\mathsf{oc}}(T) = 1 + p^d T + \dots + p^{d(m-1)}T^{m-1} + p^{dm}T^m \cdot \mathsf{Z}_{\mathfrak{g}}^{\mathsf{ask}}(T).$$

The special role of $p = 2$ reflects the fact that the p-adic exponential series $\exp(x)$ only converges for $|x|_p < p^{-1/(p-1)}$.

Corollary 5.5. *Let $p \neq 2$. Then $\mathsf{Z}_{\mathrm{GL}_d^1(\mathbf{Z}_p)}^{\mathsf{oc}}(T) = \frac{1+(p^d-2)T}{(1-T)^2}$.* ♦

Arguments similar to the proof of Proposition 5.1 allow us to compute ask zeta functions with many of the "usual suspects" among matrix Lie algebras. Recall that $\mathfrak{so}_d(R)$ denotes the Lie algebra of anti-symmetric matrices in $\mathfrak{gl}_d(R)$.

Proposition 5.6 ([17, Prop. 5.11])**.** $\mathsf{Z}_{\mathfrak{so}_d(\mathbf{Z}_p)}(T) = \mathsf{Z}_{\mathrm{M}_{d\times(d-1)}(\mathbf{Z}_p)}(T) = \frac{1-p^{1-d}T}{(1-T)(1-pT)}$.

Proof. Let $V = \mathbf{Z}_p^d$. The inclusion $\mathfrak{so}_d \hookrightarrow \mathrm{M}_d(\mathbf{Z}_p)$ is isotopic to the module representation

$$(V \wedge V)^* \xrightarrow{\theta} \mathrm{Hom}(V, V^*)$$

defined by $x(y *_\theta \psi) = (x \wedge y)\psi$, where $x, y \in V$ and $\psi \in (V \wedge V)^*$. We see that $\theta^\bullet$ is isotopic to the natural map $V \xrightarrow{\lambda} \mathrm{Hom}(V, V \wedge V)$ with $x *_\lambda y = x \wedge y$. Clearly, $V\lambda$ has constant rank $d-1$ modulo p. ♦

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 $V \wedge V \xrightarrow{0} \operatorname{Hom}(V \wedge V, V)$. 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.