Enumerating orbits of groups

Lecture 2: Ask zeta functions

Tobias Rossmann

ICTS, Bengaluru — December 2024

Ollscoil na Gaillimhe
University of Galway

Taighde Éireann
Research Ireland

Ask zeta functions v1.1

Let R be a ring. Let $M \xrightarrow{\theta} \mathrm{Hom}_R(V, W)$ be a finite free module representation. By base change, for each R-algebra S, we obtain a finite free module representation

$$M \otimes_R S \xrightarrow{\theta^S} \mathrm{Hom}_S(V \otimes_R S, W \otimes_R S).$$

Definition

The (analytic) **ask zeta function** of θ is

$$\zeta_\theta^{\mathsf{ask}}(s) = \sum_I \mathsf{ask}(\theta^{R/I}) \cdot |R/I|^{-s},$$

where the sums runs over the ideals of finite norm of R.

This generalises our previous definition of $Z_\theta^{\mathsf{ask}}(T)$. Indeed, if $R = \mathbf{Z}_p$, then

$$\zeta_\theta^{\mathsf{ask}}(s) = Z_\theta^{\mathsf{ask}}(p^{-s}).$$

Ask zeta functions v1.1

Exercise

Let $M \xrightarrow{\theta} M_{d\times e}(\mathbf{Z})$ be finite free over $\mathbf{Z}$. Then:

- $\zeta_\theta^{\mathsf{ask}}(s)$ converges for $\mathrm{Re}(s) > d+1$.
- $\zeta_\theta^{\mathsf{ask}}(s) = \prod_{p \text{ prime}} \zeta_{\theta^{\mathbf{Z}_p}}^{\mathsf{ask}}(s)$.

Using tools from p-adic integration, much more can be said about these functions.

For example:

- The abscissa of convergence $\alpha = \alpha(\theta)$ of $\zeta_\theta^{\mathsf{ask}}(s)$ is a rational number.
- For some $\delta = \delta(\theta) > 0$, the function $\zeta_\theta^{\mathsf{ask}}(s)$ admits meromorphic continuation to the half-plane $\{s \in \mathbf{C} : \mathrm{Re}(s) > \alpha - \delta\}$.
- Local functional equations / "self-reciprocity": for $p \gg 0$,

$$\left.\zeta_{\theta^{\mathbf{Z}_p}}^{\mathsf{ask}}(s)\right|_{p \leftarrow p^{-1}} = (-p^{d-s}) \cdot \zeta_{\theta^{\mathbf{Z}_p}}^{\mathsf{ask}}(s).$$

An instructive example of an ask zeta function

Motivated by probabilistic questions, Linial and Weitz (2000, unpublished) and, independently, Fulman and Goldstein (2015) proved the following.

Proposition

$\mathsf{ask}(\mathrm{M}_{d\times e}(\mathbf{F}_q)) = 1 + q^{d-e} - q^{-e}$.

The main goal of this lecture will be to prove the following.

Proposition (R. 2018)

For each prime p,

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

Our proof will rely on three tools, all of which have been very useful in the study of ask zeta functions: (1) p-adic integration, (2) constant rank spaces, and (3) Knuth duality.

An instructive example of an ask zeta function

By combining $Z^{\mathsf{ask}}_{M_{d\times e}(\mathbf{Z}_p)}(T) = \frac{1-p^{-e}T}{(1-T)(1-p^{d-e}T)}$ and the usual Euler product

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

of the Riemann zeta function, we obtain the following.

Corollary

$\zeta^{\mathsf{ask}}_{M_{d\times e}(\mathbf{Z})}(s) = \zeta(s)\zeta(s-d+e)/\zeta(s+e)$. ♦

Local ask zeta functions as integrals: motivation

- What is the size of the kernel of a matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{Z}_p)$ modulo p^n?
- We're free to multiply A by elements of $GL_2(\mathbf{Z}_p)$ on either side. Using row and column operations, we can transform A into a matrix

  $$B = \begin{bmatrix} p^\alpha & 0 \\ 0 & p^\beta \end{bmatrix}$$

  with $0 \leqslant \alpha \leqslant \beta \leqslant \infty$.
- The kernel of multiplication $\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{p^\delta} \mathbf{Z}/p^n\mathbf{Z}$ is the ideal generated by $p^{\max(n-\delta,0)}$.

  The size of this kernel is $p^{n-\max(n-\delta,0)} = p^{\min(\delta,n)}$.
- Hence, the kernel of A modulo p^n has size $p^{\min(\alpha,n)+\min(\beta,n)}$.
- Write ν for the (additive) p-adic valuation with $\nu(p) = 1$.

  Then $\alpha = \min(\nu(a), \nu(b), \nu(c), \nu(d))$ and $\alpha + \beta = \nu(\det(A))$.

Local ask zeta functions as integrals

- Let $M \xrightarrow{\theta} M_{d\times e}(\mathbf{Z}_p)$ be a finite free module representation.
- It's not surprising that $\zeta_\theta^{\mathsf{ask}}(s)$, a function defined as a series of averages, can be expressed as an integral. Here's one way of doing this.
- For $a \in M$ and $y \in \mathbf{Z}_p$, let $K_\theta(a, y) \in [1, \infty]$ be the size of the kernel of the map

$$(\mathbf{Z}_p/y\mathbf{Z}_p)^d \to (\mathbf{Z}_p/y\mathbf{Z}_p)^e$$

  induced by $a\theta$.
- Let $|\cdot|$ be the usual p-adic absolute value (on $\mathbf{Z}_p$, say) with $|p| = p^{-1}$.

Proposition (R. 2018)

For $s \in \mathbf{C}$ with $\mathrm{Re}(s) > d$,

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

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

Local ask zeta functions as integrals: minors

- We may assume that $a\theta = A(a)$ for a matrix of linear forms $A(X) \in M_{d\times e}(\mathbf{Z}_p[X])$.
- Using arguments of Voll (2010) and generalising what we did for 2×2 matrices, we can express $K_\theta(a, y)$ in terms of p-adic maximum norms of minors of $A(a)$ and y:

Lemma

Let $f_i(X)$ be the set of $i \times i$ minors of $A(X)$. 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 $y \in \mathbf{Z}_p \setminus \{0\}$,

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

Local ask zeta functions as integrals: minors

Proof.

- Fix $a \in M \setminus N$ and $y \in \mathbf{Z}_p \setminus \{0\}$. Let $n = \nu(y)$.
- 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
$$RA(a)S = \mathrm{diag}(p^{\lambda_1}, \ldots, p^{\lambda_r}, 0, \ldots, 0) =: D.$$
- 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
$$\|f_i(a)\| = p^{-\lambda_1 - \cdots - \lambda_i}.$$

Local ask zeta functions as integrals: minors

Proof (contd).

- Generalising our motivating 2×2 example, looking at D, we find that

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

- The claim follows since

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

◆

Local ask zeta functions as integrals: overview

Given $M \xrightarrow{\theta} M_{d\times e}(\mathbf{Z}_p)$, we obtained a number r and sets of polynomials $f_i(X)$ such that

$$(1-p^{-1}) \cdot \zeta_\theta^{\mathsf{ask}}(s) = \int\limits_{M\times\mathbf{Z}_p} |y|^{s+r-d-1} \prod_{i=1}^{r} \frac{\|f_{i-1}(a)\|}{\|f_i(a) \cup y f_{i-1}(a)\|} \, d\mu(a,y).$$

- While potentially unwieldy, these p-adic integrals are amenable to a wide range of tools developed over the past decades.
- Many of these tools were first pioneered in the study of *Igusa's local zeta function*.
- Key observation: when the $f_i(X)$ only consist of monomials, then our integral can be computed using techniques from polyhedral geometry.

Local ask zeta functions as integrals: consequences

Here, we just record two important consequences:

Theorem (Local rationality)

$Z^{\mathsf{ask}}_{\theta}(T) \in \mathbf{Q}(T)$. *More precisely, there are* $m \in \mathbf{N}_0$ *and nonzero* $(a_1, b_1), \ldots, (a_u, b_u) \in \mathbf{Z} \times \mathbf{N}_0$ *such that* $p^m \prod_{i=1}^{u} (1 - p^{a_i} T^{b_i}) Z^{\mathsf{ask}}_{\theta}(T) \in \mathbf{Z}[T]$.

Theorem (Variation of the prime: "(geometric) Denef formulae")

Let $M \xrightarrow{\theta} M_{d\times e}(\mathbf{Z})$ *be a finite free module representation. There are* $W_1(X, T), \ldots, W_r(X, T) \in \mathbf{Q}(X, T)$ *(which can be written over denominators of the same shape as above) and* $\mathbf{Q}$*-defined varieties* $V_1, \ldots, V_r$ *such that* $p \gg 0$,

$$Z^{\mathsf{ask}}_{\theta^{\mathbf{Z}_p}}(T) = \sum_{i=1}^{r} \# \bar{V}_i(\mathbf{F}_p) \cdot W_i(p, T),$$

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

The friendlist ask zeta functions: constant rank spaces

Definition

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

Example

Let D be a d-dimensional division algebra over F. Then the regular representation of D embeds D as a subspace of $M_d(F)$ of constant rank d.

Example (band matrices)

The following is an r-dimensional space of $r \times (2r-1)$ matrices of constant rank r:

$$B_r = \left\{ \begin{bmatrix} x_1 & x_2 & \dots & x_r & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & x_1 & x_2 & \dots & x_r \end{bmatrix} : x_1, \dots, x_r \in F \right\} \subset M_{r\times(2r-1)}(F).$$

The friendlist ask zeta functions: constant rank spaces

Proposition (R. 2018)

Let $M \subset M_{d\times e}(\mathbf{Z}_p)$ *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* $\mathbf{F}_p$*. (Same* r*!)*
Then

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

The friendlist ask zeta functions: constant rank spaces

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 $K_M(a,y)$ to the case that $a \in M \setminus pM$.
  Key observation: $K_M(pa, py) = p^d\, K(a,y)$.
  This leads to
  $$(1 - p^{d-\ell-s}) \cdot \zeta_M^{\mathsf{ask}}(s) = 1 + (1-p^{-1})^{-1} \int_{(M\setminus pM)\times p\mathbf{Z}_p} |y|^{s-1}\, K_M(a,y)\, d\mu(a,y).$$
- For $a \in M \setminus pM$, since $\bar{M}$ has constant rank r, $K_M(a,p) = p^{d-r}$ and, more generally,
  $$K_M(a,y) = |y|^{r-d}$$
  for all $y \in \mathbf{Z}_p \setminus \{0\}$.
- Evaluating our integral is now straightforward. :) ♦

Hidden constant rank spaces?

We just proved this:

Proposition

Let $M \subset M_{d\times e}(\mathbf{Z}_p)$ *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*

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

I promised to prove the following:

Proposition

$$\mathsf{Z}^{\mathsf{ask}}_{M_{d\times e}(\mathbf{Z}_p)}(T) = \frac{1 - p^{-e}T}{(1-T)(1-p^{d-e}T)}.$$

Suspiciously similar formulae. . . even though $M_{d\times e}(\mathbf{Z}_p)$ is about as far from having constant rank as you can get!

Knuth duality (or: matrix transposes turned up to 11)

- Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation over R.
- 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'll spell this out for 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:

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

Knuth duality (or: matrix transposes turned up to 11)

Example

Let $A(X) \in M_{d\times e}(R[X_1, \ldots, X_\ell])$ be a matrix of linear forms, say

$$A(X) = \left[\sum_{h=1}^{\ell} c_{hij} X_h\right]_{ij}.$$

Up to isotopy, $\circ$, $\bullet$, and $\vee$ are the involutions permuting our three "axes". In detail:

- $A(X)^\circ$ is the $\ell \times e$ matrix with (h, j) entry $\sum_{i=1}^{d} c_{hij} X_i$.
- $A(X)^\bullet$ is the $d \times \ell$ matrix with (i, h) entry $\sum_{j=1}^{e} c_{hij} X_j$.
- $A(X)^\vee = A(X)^\top$ is just the transpose of $A(X)$.

For $\ell = d = e$, this is the setting considered by Knuth (1965) in the study of *semifields*.

Knuth duality (or: matrix transposes turned up to 11)

Theorem (R. 2020)

Let R be a finite quotient of a Dedekind domain (e.g. $R = \mathbf{Z}/n\mathbf{Z}$).
Let $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ be a module representation over R.
Suppose that M, V, and W are finite. Then:

- $\mathsf{ask}(\theta^\circ) = \frac{|M|}{|V|}\mathsf{ask}(\theta)$.
- $\mathsf{ask}(\theta^\bullet) = \mathsf{ask}(\theta)$.
- $\mathsf{ask}(\theta^\vee) = \frac{|W|}{|V|}\mathsf{ask}(\theta)$.

Corollary

Let $\mathbf{Z}_p^\ell \approx M \xrightarrow{\theta} M_{d\times e}(\mathbf{Z}_p)$ be a module representation over $\mathbf{Z}_p$. Then:

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

♦

Knuth duality (or: matrix transposes turned up to 11)

Proof of theorem.

- We'll only prove the first part. This only needs $|R| < \infty$ and goes back to an unpublished note of Linial and Weitz (2020) mentioned before.
- Let
$$\Sigma(\theta) = \{(x, a) \in V \times M : x *_\theta a = 0\}$$
and note that $(x, a) \in \Sigma(\theta)$ if and only if $(a, x) \in \Sigma(\theta^\circ)$.
- Clearly, $\mathsf{ask}(\theta) = \frac{|\Sigma(\theta)|}{|M|}$.
- Hence,
$$\mathsf{ask}(\theta^\circ) = \frac{|\Sigma(\theta^\circ)|}{|V|} = \frac{|\Sigma(\theta)|}{|V|} = \frac{|M|}{|V|}\mathsf{ask}(\theta).$$

This was the same argument as in the proof of the orbit-counting lemma! ♦

Ask zeta functions of generic matrices

We can now finally prove the following:

Proposition

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

Sketch of proof.

- Over a field F, the $\circ$-dual of the identity map $\mathrm{M}_{d\times e}(F) \to \mathrm{Hom}(F^d, F^e)$ is

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

- By playing with the standard basis of $\mathrm{M}_{d\times e}(F)$, we see that $A \mapsto xA$ is onto for each nonzero $x \in F^d$.
- Hence, our $\circ$-dual parameterises a space of constant rank e.
- Now apply our earlier results on ask zeta functions of $\circ$-duals and those of constant rank spaces. ♦

Ask zeta functions of generic matrices

Proof (less sketchy).

- Let ι be the identity on $\mathrm{M}_{d\times e}(\mathbf{Z}_p)$, viewed as a module representation $\mathrm{M}_{d\times e}(\mathbf{Z}_p) \to \mathrm{Hom}(\mathbf{Z}_p^d, \mathbf{Z}_p^e)$.
- We obtain $\mathbf{Z}_p^d \xrightarrow{\iota^\circ} \mathrm{Hom}(\mathrm{M}_{d\times e}(\mathbf{Z}_p), \mathbf{Z}_p^e), \quad x \mapsto (A \mapsto xA)$.
- Considering the same module representation over a field, if $x \neq 0$, then $A \mapsto xA$ is onto. Hence, $\iota^\circ \bmod p$ parameterises a space of matrices of constant rank e.
- Hence, using our earlier theorem (with (d, e, de, e) in place of (ℓ, r, d, e)) yields

$$\mathsf{Z}^{\mathsf{ask}}_{\iota^\circ}(T) = \frac{1 - p^{de-d-e}T}{(1 - p^{de-d}T)(1 - p^{de-e}T)}.$$

- Thus, finally,

$$\mathsf{Z}^{\mathsf{ask}}_{\mathrm{M}_{d\times e}(\mathbf{Z}_p)}(T) = \mathsf{Z}^{\mathsf{ask}}_{\iota}(T) = \mathsf{Z}^{\mathsf{ask}}_{\iota^\circ}(p^{d-de}T) = \frac{1 - p^{-e}T}{(1 - T)(1 - p^{d-e}T)},$$

as claimed. ♦

Further examples

Similar reasoning applies to many of the "usual suspects" among modules of matrices. Recall the definitions of the **special linear**, **orthogonal**, and **symplectic** Lie algebras

$$\mathfrak{sl}_d(R) = \left\{a \in \mathfrak{gl}_d(R) : \mathrm{trace}(a) = 0\right\},$$

$$\mathfrak{so}_d(R) = \left\{a \in \mathfrak{gl}_d(R) : a + a^\top = 0\right\}, \quad \text{and}$$

$$\mathfrak{sp}_{2d}(R) = \left\{\begin{bmatrix} a & b \\ c & -a^\top \end{bmatrix} : a, b, c \in M_d(R), b = b^\top, c = c^\top\right\}.$$

Further examples

Proposition (R. 2018)

- $Z^{\mathsf{ask}}_{\mathfrak{sl}_d(\mathbf{Z}_p)}(T) = Z^{\mathsf{ask}}_{\mathfrak{gl}_d(\mathbf{Z}_p)}(T) = \frac{1-p^{-d}T}{(1-T)^2}$ *(for $d > 1$).*
- $Z^{\mathsf{ask}}_{\mathfrak{so}_d(\mathbf{Z}_p)}(T) = Z^{\mathsf{ask}}_{\mathrm{M}_{d\times(d-1)}(\mathbf{Z}_p)}(T) = \frac{1-p^{1-d}T}{(1-T)(1-pT)}$.
- $Z^{\mathsf{ask}}_{\mathfrak{sp}_{2d}(\mathbf{Z}_p)}(T) = Z^{\mathsf{ask}}_{\mathfrak{gl}_{2d}(\mathbf{Z}_p)}(T) = \frac{1-p^{-2d}T}{(1-T)^2}$.
- $Z^{\mathsf{ask}}_{\mathfrak{n}_d(\mathbf{Z}_p)}(T) = \frac{(1-T)^{d-1}}{(1-pT)^d}$.

- All but the last of these examples are explained by hidden constant rank spaces.
- We nowadays understand such coincidences between ask zeta functions much better. In particular:
  - The fact that $\mathfrak{gl}_d(\mathbf{Z}_p)$ and $\mathfrak{sl}_d(\mathbf{Z}_p)$ have the same ask zeta function is an instance of a more general phenomenon: the rigidity of ask zeta functions under imposing suitably "admissible" linear relations (Carnevale & R. 2022).
  - The fact that $\mathfrak{so}_d(\mathbf{Z}_p)$ and $\mathrm{M}_{d\times(d-1)}(\mathbf{Z}_p)$ have the same ask zeta function is a special case of the "Cograph Modelling Theorem" (R. & Voll 2024).