Enumerating orbits of groups

Lecture 3: A web of themes and open problems

Tobias Rossmann

ICTS, Bengaluru — December 2024

Ollscoil na Gaillimhe
University of Galway

Taighde Éireann
Research Ireland

CC BY

Theme: tame vs wild

Given an instance of a global (say $\mathbf{Z}$-defined) counting problem with local zeta functions $Z_p(T)$ (p prime), we regard our instance as *tame* if there exists a rational function $W(X, T)$ such that $Z_p(T) = W(p, T)$ for $p \gg 0$.

This is often referred to as *(almost) uniformity*. In the study of p-adic integrals, model theorists use the term "uniformity" to mean something else, which can be confusing.

Example

The local class-counting zeta functions of the Heisenberg group are given by the uniform formula

$$Z^{\mathsf{cc}}_{\mathrm{U}_3 \otimes \mathbf{Z}_p}(T) = \frac{1 - T}{(1 - pT)(1 - p^2 T)}.$$

Hence, counting conjugacy classes of $\mathrm{U}_3(\mathbf{Z}/p^n\mathbf{Z})$ is tame.

Theme: tame vs wild

- Informally, we regard a counting problem as *(geometrically) wild* if, by varying over all or some instances, the behaviour of $Z_p(T)$ as p varies captures the numbers of $\mathbf{F}_p$-rational points on arbitrary ($\mathbf{Z}$-defined) schemes.
- Many counting problems of interest are *at most* geometrically wild. More precisely, they often admit *(geometric) Denef formulae*, valid for $p \gg 0$, of the form

$$Z_p(T) = \sum_{i=1}^{r} \#V_i(\mathbf{F}_p) \cdot W_i(p, T)$$

  for schemes V_i and rational functions $W_i(X, T)$.
- Known tame counting problems are often *combinatorial*, while wild ones are *(algebro-)geometric*.
- When instances of counting problems are tame, we can seek to find combinatorial (or other) reasons for that by e.g. showing that $\#V_i(\mathbf{F}_p) \in \mathbf{Q}[p]$ for $p \gg 0$.
- Proving or exhibiting instances of wild behaviour is a very different kind of problem. Far fewer tools have been developed for this purpose.

Average sizes of kernels and enumerating matrices by rank

- Let $A(X) \in \mathrm{M}_{d\times e}(\mathbf{Z}[X_1,\dots,X_\ell])$ be a matrix of linear forms, corresponding to a module representation $\theta\colon \mathbf{Z}^\ell \to \mathrm{M}_{d\times e}(\mathbf{Z}), \quad x \mapsto A(x)$.
- Let V_i be the "rank-i locus" of $A(X)$.

  This is the part of affine ℓ-space where all $(i+1)\times(i+1)$ minors of $A(X)$ vanish, but some $i\times i$ minor is invertible.
- We then have $\mathsf{ask}(\theta^{\mathbf{F}_q}) = \sum_{i=0}^{\infty} \#V_i(\mathbf{F}_q) q^{d-i-\ell}$.
- Hence, for fixed θ, the study of $\mathsf{ask}(\theta^{\mathbf{F}_q})$ as q varies is at most as hard as counting $\mathbf{F}_q$-rational points on schemes.
- Polynomiality questions surrounding rank counts in combinatorially-defined spaces of matrices have been of considerable interest for a *long* time.

  Some papers: Landsberg 1893, Carlitz 1954, MacWilliams 1969, Buckhiester 1972, Bender 1974, Lewis et al. 2011, Klein et al. 2014

Wild problems

- Recall that we regard a counting problem depending on a prime p or prime power q as *geometrically wild* if it is at least as hard as counting $\mathbf{F}_p$- or $\mathbf{F}_q$-points on arbitrary schemes.
- Belkale and Brosnan (2003) showed the following:

  Counting invertible symmetric $n \times n$ matrices over $\mathbf{F}_q$ with entries in specified positions forced to be zero is a wild problem.

  (More precise version below!)
- I'm not aware of results of this type which prove wildness for zeta functions of algebraic structures.
- However, if we're willing to settle for a weaker "approximate form" of wildness, then the following result takes care of ask, class-counting, and orbit-counting zeta functions.

Approximate wildness

Theorem (R. 2024)

Let X be a scheme of finite type over $\mathbf{Z}$. Let $n \geqslant 1$. Then there are

- *commutative group schemes $M_1, \dots, M_r$ with $M_i \leqslant U_{d_i}$,*
- *Baer group schemes $G_1, \dots, G_r$, and*
- *univariate Laurent polynomials $f_1, \dots, f_r, g_1, \dots, g_r$ over $\mathbf{Z}$*

such that for each prime power q, the numbers

$$F(q) := \sum_{i=1}^{r} f_i(q)\, k(G_i(\mathbf{F}_q)) \text{ and } G(q) := \sum_{i=1}^{r} g_i(q)\, \#(\mathbf{F}_q^{d_i}/M_i(\mathbf{F}_q))$$

are integers which satisfy

$$\boxed{\#X(\mathbf{F}_q) \equiv F(q) \equiv G(q) \pmod{q^n}.}$$

Given X, there exists n with $\#X(\mathbf{F}_q) < q^n$ for all q. Hence: class numbers and numbers of orbits of unipotent groups are *"at least as complicated"* as numbers of $\mathbf{F}_q$-rational points on arbitrary schemes. We already saw that they're at most this complicated.

Kontsevich's conjecture

Let $\Gamma = (V, E)$ be a graph.

Definition

The *Kirchhoff polynomial* of Γ is

$$P_\Gamma(X) = \sum_T \prod_{e \notin T} X_e,$$

where the sum ranges over spanning trees of Γ.

Conjecture (Kontsevich)

For each Γ, the number of solutions of $P_\Gamma(X) = 0$ (in $\mathbf{A}^E$) over $\mathbf{F}_q$ is given by a polynomial in q.

Kontsevich's conjecture

Theorem (Belkale and Brosnan 2003)

Kontsevich's conjecture is maximally false: counting $\mathbf{F}_q$-points of $P_\Gamma(X) = 0$ as Γ ranges over graphs is as hard as counting $\mathbf{F}_q$-points on arbitrary schemes over $\mathbf{Z}$.

- Let Γ be a graph with distinct vertices $v_1, \ldots, v_n$.
- Let $M_\Gamma^+ = [x_{ij}]$ be the generic symmetric $n \times n$ matrices with $x_{ij} = 0$ for $v_i \sim v_j$.
- Let Z_Γ be the regular locus of M_Γ^+.
- As part of numerous clever translations and (equally clever!) reductions, Belkale and Brosnan showed that the counting functions

$$q \mapsto \#Z_\Gamma(\mathbf{F}_q)$$

generate (a certain localisation of) the algebra of all point-counting functions derived from schemes over $\mathbf{Z}$.

Wild Baers

We can use this result to construct Baer group schemes with “approximately wild” numbers of conjugacy classes as in our theorem.

- Given Γ, consider
$$A_\Gamma = \begin{bmatrix} 0 & M_\Gamma^+ \\ -(M_\Gamma^+)^\top & 0 \end{bmatrix}.$$
- This is an antisymmetric matrix of linear forms (over $\mathbf{Z}$) which gives rise to an alternating bilinear map $*$.
- The Baer group schemes with “wild mod q^n” numbers of conjugacy classes are iterated central powers of the $\mathbf{G}_*$—the number of factors depends on n.

Class-counting zeta functions of graphical groups: tame or wild?

How do class-counting zeta functions of graphical group schemes $\mathbf{G}_\Gamma$ look like?

- These zeta functions can be expressed in terms of the rank loci of generic antisymmetric matrices with support constraints.
- Inspired by the work of Belkale and Brosnan, this motivated R. & Voll to suspect that graphical group schemes have wild class-counting zeta functions.
- After all... how likely is it that wild pieces add up to something tame (polynomial)?

$\sum$ wild = tame, sometimes

Example (Carnevale & R. 2022)

- Let

$$M = \{[x_{ij}] \in M_3(\mathbf{Z}) : x_{11} + x_{33} = x_{12} + x_{21} = x_{13} + x_{22} + x_{32} = x_{23} + x_{31} = 0\}.$$

- We can consider the group scheme $\mathbf{G}_M \leqslant \mathrm{GL}_6$ (see the tutorial).
- There are $q^3 - q$ orbits of size q^3, $q^2 - q$ orbits of size q^2, and q^3 fixed points of $\mathbf{G}_M(\mathbf{F}_q)$ acting on $\mathbf{F}_q^6$.
- The number of elements of $\mathbf{G}_M(\mathbf{F}_q)$ with precisely q^5 fixed points on $\mathbf{F}_q^6$ is not quasi-polynomial.

  This number is $(q-1)(N(q)+1)$, where $N(q)$ is the number of roots of $X^5 + X - 1$ in $\mathbf{F}_q$.
- By taking Knuth duals, the roles of orbit and fixed point set sizes can be interchanged.

The Uniformity Theorem

It turns out that class-counting zeta functions of graphical groups are tame:

Theorem (R. & Voll 2024)

Let Γ be a graph with m edges. There exists $W_\Gamma(X,T) \in \mathbf{Q}(X,T)$ such that for each prime p,

$$Z^{cc}_{\mathbf{G}_\Gamma \otimes \mathbf{Z}_p}(T) = W_\Gamma(p, p^m T).$$

(We could of course absorb the factor p^m and just consider $W_\Gamma(X, X^m T)$ instead. We would then have to adjust some of the formulae and identities below.)

Remark

- Our proof is constructive and implemented in Zeta. It is based on a (quite elaborate) recursion which uses *toric geometry* to analyse p-adic integrals attached to ask zeta functions.
- A list of these rational functions for graphs on at most 7 vertices is available online.
- Some infinite families have received special attention.

Theme: rigidity of ask zeta functions

- In the study of ask zeta functions, one cannot help but notice examples of different module representations giving rise to the same zeta functions.
- Earlier example: $\mathfrak{gl}_d(\mathbf{Z}_p)$ and $\mathfrak{sl}_d(\mathbf{Z}_p)$ have the same ask zeta functions for $d > 1$.
- (Carnevale & R. 2022): More generally, certain *admissible* linear relations have no effect on ask zeta functions. The following is a fun application of this theme.
- Let $\mathsf{F}_{c,d}$ be the group scheme associated with the free nilpotent Lie algebra of class c and rank d. Example: $\mathsf{F}_{2,2} = \mathrm{U}_3$

  $\mathsf{F}_{c,d}$ can be defined by exponentiating the corresponding relatively free Lie algebra over $\mathbf{Z}[1/c!]$. For $p > c$, the group $\mathsf{F}_{c,d}(\mathbf{Z}_p)$ is the free nilpotent pro-p group of class c on d generators.

Theme: rigidity of ask zeta functions

Theorem (Lins 2020)

$$Z^{cc}_{F_{2,d}\otimes \mathbf{Z}_p}(T) = \frac{1 - p^{\binom{d-1}{2}}T}{(1-p^{\binom{d}{2}}T)(1-p^{\binom{d}{2}+1}T)}.$$

Two further proofs are known at this point.

The proof of the following theorem fits the theme of rigidity.

Theorem (Carnevale & R. 2022)

Let $p \geqslant 5$. *Then:*

$$Z^{cc}_{F_{3,d}\otimes \mathbf{Z}_p}(T) = \frac{\left(1-p^{\frac{(d-1)(d^2+d-3)}{3}}T\right)\left(1-p^{\frac{(d-2)d(d+2)}{3}}T\right)}{\left(1-p^{\frac{(d-1)d(d+1)}{3}}T\right)\left(1-p^{\frac{d^3-d+3}{3}}T\right)\left(1-p^{\frac{(2d^2+3d-11)d}{6}}T\right)}.$$

Theme: rigidity of ask zeta functions

Sketch of proof.

- Let $\mathfrak{a}_{c,d}$ be the free algebra generated by d symbols subject to the relations $x^2 = 0$ and $x_1(x_2(\cdots(x_c x_{c+1})\cdots)) = 0$.
- Let $\mathfrak{f}_{c,d} = \mathfrak{a}_{c,d}/(\text{Jacobi identity})$, the free class-$c$ nilpotent Lie algebra of rank d.
- Let $\alpha_{c,d}$ (resp. $\hat{\alpha}_{c,d}$) be the $\bullet$-dual of the adjoint representation of $\mathfrak{a}_{c,d}$ (resp. $\mathfrak{f}_{c,d}$).
- General ask machinery: $Z^{\mathsf{cc}}_{\mathsf{F}_{c,d}\otimes\mathbf{Z}_p}(T) = Z^{\mathsf{ask}}_{\hat{\alpha}^{\mathbf{Z}_p}_{c,d}}(T)$.
- The ask zeta function of a module representation arising from a matrix of linear forms $A(X)$ is determined by the sequence of *Fitting ideals* of $\mathrm{Coker}(A(X))$.

  These are the ideals of minors of $A(X)$, ordered in a certain way.
- Induction and a Gröbner basis calculation (using Macaulay2 or SageMath) show that for $c = 3$, our two module representations $\alpha_{3,d}$ and $\hat{\alpha}_{3,d}$ give rise to the <u>same</u> Fitting ideals. Hence, $Z^{\mathsf{cc}}_{\mathsf{F}_{3,d}\otimes\mathbf{Z}_p}(T) = Z^{\mathsf{ask}}_{\alpha^{\mathbf{Z}_p}_{3,d}}(T)$.
- The latter zeta functions turns out to (essentially) coincide with the class-counting zeta function of graphical group schemes attached to so-called threshold graphs. We can then read off our formula from known work (R. & Voll 2024). :) ♦

Theme: rigidity of ask zeta functions

- It seems that we are only beginning to understand rigidity phenomena. Here is another example. Let $\Gamma = (V, E)$ be a simple graph with vertices $v_1, \ldots, v_n$.
- Let $M_\Gamma = \{[x_{ij}] \in M_n(\mathbf{Z}) : x_{ij} = 0 \text{ if } v_i \sim v_j\}$.
- Let M_Γ^+ (M_Γ^-) consist of the symmetric (resp. antisymmetric) matrices in M_Γ.

Theorem (R. & Voll 2025+)

$\mathsf{Z}^{\mathsf{ask}}_{\mathbf{Z}_p M_\Gamma}(T) = \mathsf{Z}^{\mathsf{ask}}_{\mathbf{Z}_p M_\Gamma^-}(T) = \mathsf{Z}^{\mathsf{ask}}_{\mathbf{Z}_p M_\Gamma^+}(T)$ *(where the second equality needs $p > 2$.)*

Example

Taking $\Gamma =$ •—•—•, the theorem e.g. explains why $\left\{ \begin{bmatrix} a & 0 & b \\ 0 & c & 0 \\ d & 0 & e \end{bmatrix} : a, b, c, d, e \in \mathbf{Z}_p \right\}$ and its submodule $\left\{ \begin{bmatrix} a & 0 & b \\ 0 & c & 0 \\ -b & 0 & e \end{bmatrix} : a, b, c, e \in \mathbf{Z}_p \right\}$ have the same ask zeta function.

The common ask zeta function is $\frac{1+T-2q^{-1}T-2q^{-2}T+q^{-3}T+q^{-3}T^2}{(1-T)^3}$, in case you were wondering.

Theme: modelling theorems

- A **hypergraph** is a triple $H = (V, E, \imath)$ consisting of finite sets V and E and an **incidence relation** $\imath \subset V \times E$. The elements of V and E are the **vertices** and **hyperedges** of H, respectively.
- Let $V = \{v_1, \ldots, v_n\}$ and $E = \{e_1, \ldots, e_m\}$. Let M_H be the module of $n \times m$ matrices $[x_{ij}]$ over $\mathbf{Z}$ with $x_{ij} = 0$ unless $v_i \,\imath\, e_j$.
- The **support** of a hyperedge e is $\|e\| = \{v \in V : v \,\imath\, e\}$.
- Let $\widehat{\mathrm{WO}}(V)$ be the poset of (possibly empty) flags of (possibly empty) subsets of V.
- Let $\mu_I = \mu_I(H)$ be the number of hyperedges e with $\|e\| = I$. Define

$$I_H(X, T) = \sum_{y \in \widehat{\mathrm{WO}}(V)} (1 - X^{-1})^{|\sup(y)|} \prod_{J \in y} \frac{X^{|J| - \sum_{I : I \cap J \neq \emptyset} \mu_I} T}{1 - X^{|J| - \sum_{I : I \cap J \neq \emptyset} \mu_I} T}.$$

Theorem (R. Voll 2024)

$Z^{\mathrm{ask}}_{\mathbf{Z}_p M_H}(T) = I_H(p, T)$ *for each prime* p.

Theme: modelling theorems

Definition

Cographs are recursively defined as follows:

- A graph consisting of a single vertex is a cograph.
- If Γ and Γ' are cographs, then so are their disjoint union $\Gamma \oplus \Gamma'$ and their join $\Gamma \vee \Gamma'$.

  The join $\Gamma_1 \vee \Gamma_2$ is obtained from $\Gamma_1 \oplus \Gamma_2$ by connecting each vertex of Γ_1 to each vertex of Γ_2.

Theorem (“Cograph modelling theorem”; R. & Voll 2024)

Let Γ be a cograph. Then there exists an explicit ***modelling hypergraph*** $\mathsf{H} = \mathsf{H}(\Gamma)$ *with $W_\Gamma(X, T) = I_{\mathsf{H}}(X, T)$.*

The point is that we have an explicit *combinatorial Denef formula* for $I_{\mathsf{H}}(X, T)$ which then allows us to deduce properties of $W_\Gamma(X, T)$ and hence of class-counting zeta functions of cographical groups. Consequences include:

- If Γ is a cograph, then the abscissa of convergence of $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma}(s)$ is an integer.
- If Γ is a cograph, then each real pole of $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma \otimes \mathbf{Z}_p}(s)$ is an integer.

Theme: operations

- An attractive feature of ask zeta functions, and hence of class- and orbit-counting zeta functions of unipotent groups, is that they are often well behaved w.r.t. algebraic operations.
- Knuth duality (and its harmless effects on ask zeta functions) are one example.
- Given module representation $M \xrightarrow{\theta} \mathrm{Hom}(V, W)$ and $M' \xrightarrow{\theta'} \mathrm{Hom}(V', W')$, we obtain

$$M \oplus M' \xrightarrow{\theta \oplus \theta'} \mathrm{Hom}(V \oplus V', W \oplus W').$$

- Recall that the **Hadamard product** of $F(T) = \sum_{n=0}^{\infty} a_n T^n$ and $G(T) = \sum_{n=0}^{\infty} b_n T^n$ is

$$F(T) *_T G(T) = \sum_{n=0}^{\infty} a_n b_n T^n.$$

- It is well known that Hadamard products of rational generating functions are themselves rational.

Hadamard products

Lemma

Let θ *and* θ' *be finite free module representations over* $\mathbf{Z}_p$*.*
Then $\mathsf{Z}^{\mathsf{ask}}_{\theta\oplus\theta'}(T) = \mathsf{Z}^{\mathsf{ask}}_{\theta}(T) *_T \mathsf{Z}^{\mathsf{ask}}_{\theta'}(T)$*.* ♦

Lemma

Let $\mathbf{G}$ *and* $\mathbf{G}'$ *be group schemes over* $\mathbf{Z}_p$*. Then* $\mathsf{Z}^{\mathsf{cc}}_{\mathbf{G}\times\mathbf{G}'}(T) = \mathsf{Z}^{\mathsf{cc}}_{\mathbf{G}}(T) *_T \mathsf{Z}^{\mathsf{cc}}_{\mathbf{G}'}(T)$*.*

Proof.

We have $k(G \times G') = k(G)\,k(G')$ for finite groups G and G'. ♦

- Already for examples of the form $M_{d\times e}(\mathbf{Z}_p)$, the study of Hadamard products of ask zeta functions very naturally touches upon and involves *permutation statistics*.
- We saw some glimpses of that in the tutorial.
- More about this: see Angela's third lecture. :)

Joins of graphs

Theorem (R. & Voll 2025+)

Let Γ_1 and Γ_2 be graphs on n_1 and n_2 vertices, respectively. Then

$$\begin{aligned} W_{\Gamma_1 \vee \Gamma_2}(X,T) = \big(&X^{1-n_1-n_2}T - 1 \\ &+ W_{\Gamma_1}(X, X^{-n_2}T)(1 - X^{-n_2}T)(1 - X^{1-n_2}T) \\ &+ W_{\Gamma_2}(X, X^{-n_1}T)(1 - X^{-n_1}T)(1 - X^{1-n_1}T)\big) \\ &/((1-T)(1-XT)). \end{aligned}$$

Remark

In the special case that Γ_1 and Γ_2 are *cographs*, this was first proved by R. & Voll (2024). (This used the Cograph Modelling Theorem.)

It remains open to conceptually understand the above product of generating functions.

Open problem: Hadamard products

- At this point, we have a combinatorial understanding of Hadamard products

$$\mathsf{Z}^{\mathsf{ask}}_{\mathrm{M}_{d_1 \times e_1}(\mathbf{Z}_p)} *_{\mathsf{T}} \cdots *_{\mathsf{T}} \mathsf{Z}^{\mathsf{ask}}_{\mathrm{M}_{d_r \times e_r}(\mathbf{Z}_p)}$$

  when $d_1 - e_1 = \cdots = d_r - e_r$ in terms of shuffles of coloured permutations (Carnevale, Moustakas, R. 2024+).
- This is e.g. sufficient to explicitly determine the class-counting zeta functions of $\mathsf{F}_{2,d_1} \times \cdots \times \mathsf{F}_{2,d_r}$.

Problem

Given arbitrary (d_i, e_i), provide a useful combinatorial interpretion of the above rational generating function.

Open problem: free nilpotent groups

Question

Let $c \geqslant 4$.

- Does there exist $W_{c,d}(X,T) \in \mathbf{Q}(X,T)$ with $Z^{cc}_{F_{c,d}\otimes \mathbf{Z}_p}(T) = W_{c,d}(p,T)$ for $p \gg 0$?
- If so, how does $W_{c,d}(X,T)$ look like?

- We saw that the answer is YES for $c = 2$ and $c = 3$ (and any d).
- O'Brien & Voll (2015) explicitly determined the number of conjugacy classes of given size of $F_{c,d}(\mathbf{F}_q)$ in terms of Witt's dimension formula. This takes care of the coefficient of T in $Z^{cc}_{F_{c,d}\otimes \mathbf{Z}_p}(T)$.
- Contrary to what happens for $c = 2, 3$, we shouldn't expect formulae of the form $\prod(1 - p^{a_i}T^{b_i})^{\pm 1}$. Indeed:

$$Z^{cc}_{F_{4,2}\otimes \mathbf{Z}_p}(T) = \frac{p^7T^3 - p^6T^2 - p^5T^2 + p^4T^2 + p^3T - p^2T - pT + 1}{(1-p^7T^2)(1-p^4T)^2}.$$

Open problem: class-counting zeta functions of graphical groups

Given n, using the Cograph Modelling Theorem and the Uniformity Theorem for hypergraphs, we can produce an explicit combinatorial Denef formula (specifically: a sum over flags of subsets of $\{1, \ldots, n\}$) for the rational functions $W_\Gamma(X, T)$ attached to cographs on n vertices.

Question (R. & Voll 2024)

Let Γ be a simple graph.

1. Is the abscissa of convergence of $\zeta^{cc}_{\mathbf{G}_\Gamma}(s)$ always an integer?
2. Are the real parts of the poles of $\zeta^{cc}_{\mathbf{G}_\Gamma \otimes \mathbf{Z}_p}(s)$ always half-integers?
3. Is there a meaningful "combinatorial Denef formula" for the $W_\Gamma(X, T)$ which is valid for *all* graphs on a given vertex set?

The End.

Thank you!

Compiled on 2024-12-06 at 08:55:56 UTC.