Tensors and Group Orbits

Wild, tame, wild, tame, ...

Ollscoil na Gaillimhe
University of Galway

Tobias Rossmann

Pfaffians, Tensors, and Applications, MPI Leipzig

November 2022

Symbolic enumeration

Problem (template)

Enumerate *"things"* (e.g. groups, graphs, ...) depending on a parameter (e.g. order) up to their *"symmetries"* as a *"symbolic function"* of the parameter.

Problem (friendly instance)

Given a group scheme $\mathbf{G}$ acting on a scheme $\mathbf{X}$, enumerate the orbits of $\mathbf{G}(R)$ on $\mathbf{X}(R)$ as R ranges over interesting families of rings (e.g. finite fields).

Definition

$$\mathrm{U}_n = \begin{bmatrix} 1 & * & \ldots & \ldots & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & * \\ 0 & \ldots & \ldots & 0 & 1 \end{bmatrix} \leqslant \mathrm{GL}_n$$

Example (linear orbits)

- Obvious: $\mathrm{GL}_n(\mathbf{F}_q)$ has two orbits on $\mathbf{F}_q^n$ for $n \geqslant 1$, independently of q.
- Exercise: $\mathrm{U}_n(\mathbf{F}_q)$ has precisely $nq - n + 1$ orbits on $\mathbf{F}_q^n$.

Conjugacy classes

Definition

Let G be a group.

- **Conjugate elements:** $g \sim h \Leftrightarrow g = x^{-1}hx \text{ for some } x$
- **Conjugacy classes:** equivalence classes w.r.t. $\sim$.
- **Class number** $\mathrm{k}(G)$: no. of conjugacy classes

Example (matrices)

- Conjugacy classes in $\mathrm{GL}_n(\mathbf{C}) \leftrightarrow$ Jordan normal forms.
- $\mathrm{k}(\mathrm{GL}_n(\mathbf{F}_q))$ is a polynomial in q.

  See e.g. Stanley's "Enumerative Combinatorics" (Vol. 1), Exercise 1.190.

Higman's conjecture

Conjecture

(G. Higman 1960)

$\mathrm{k}(\mathrm{U}_n(\mathbf{F}_q))$ is a polynomial in q.

Higman's conjecture

> *"[...] it would also be interesting to know whether, as a consideration of small values of n suggests, for fixed n the class number is a polynomial in q"*
>
> — G. Higman

Conjecture

(G. Higman 1960)

$\mathbf{k}(\mathrm{U}_n(\mathbf{F}_q))$ is a polynomial in q.

Example

$\mathrm{k}(\mathrm{U}_3(\mathbf{F}_q)) = q^2 + q - 1.$

Theorem

(Vera-López & Arregi 2003,
Pak & Soffer 2015$^+$)

Higman's conjecture is true for $n \leqslant 16$.

Related work

Polynomiality questions for other families of (unipotent) groups: Evseev, Goodwin, Isaacs, Le, Lehrer, Magaard, Röhrle ...

Families of rings and groups

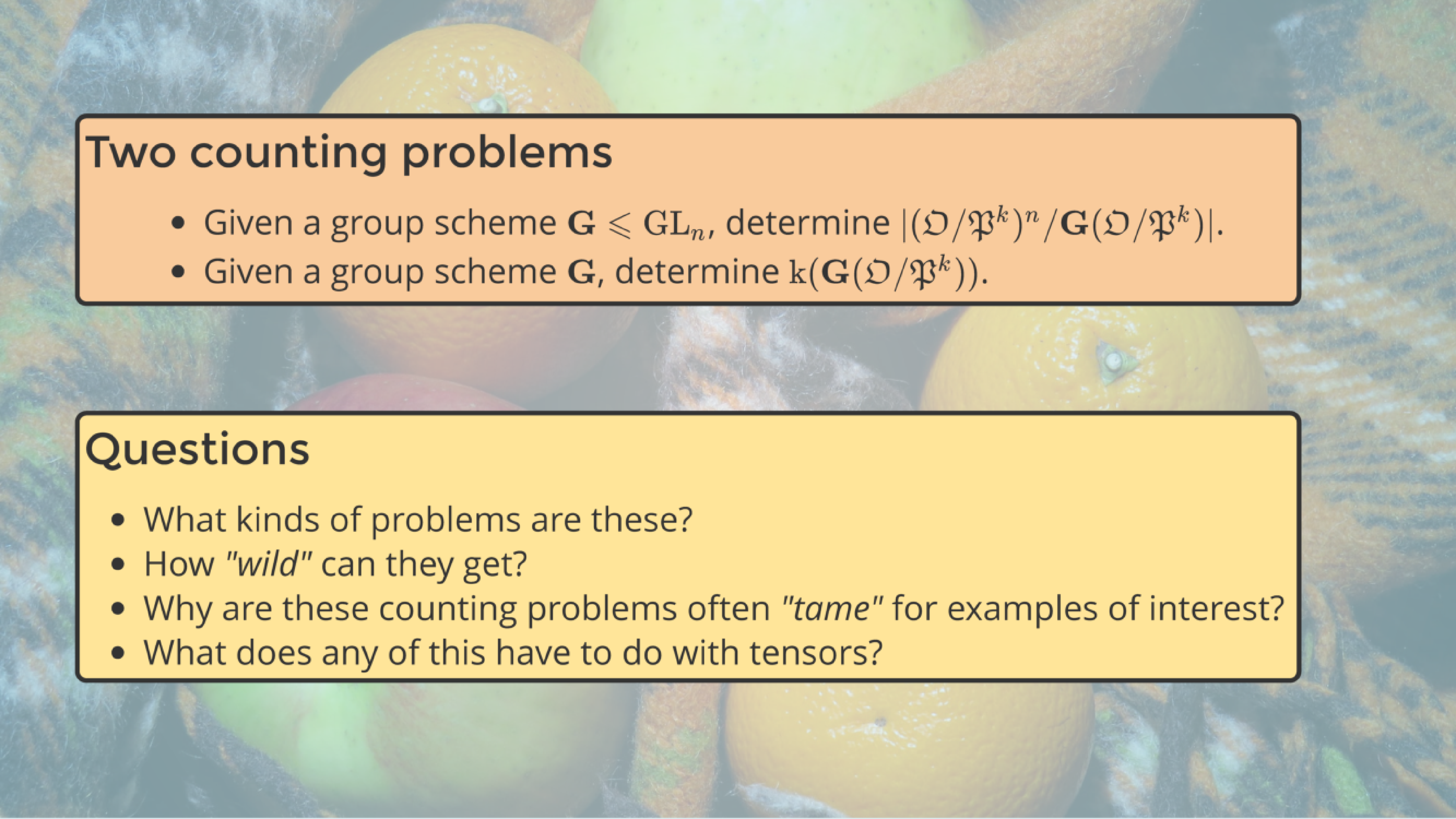
Given a unipotent group scheme $\mathbf{G} \leqslant \mathrm{U}_n$, we obtain finite p-groups $\mathbf{G}(\mathbf{F}_{p^k})$ and $\mathbf{G}(\mathbf{Z}/p^k\mathbf{Z})$.

Simultaneous generalisation

For a compact discrete valuation ring (DVR) $\mathfrak{O}$ with maximal ideal $\mathfrak{P}$, we obtain p-groups $\mathbf{G}(\mathfrak{O}/\mathfrak{P}^k)$, where $p = \mathrm{char}(\mathfrak{O}/\mathfrak{P})$.

Compact DVRs come in two flavours.

- Characteristic zero:
  Valuation rings of finite extensions of $\mathbf{Q}_p$, e.g. $\mathbf{Z}_p$.
- Positive characteristic:
  Formal power series rings $\mathbf{F}_q[\![z]\!]$.



Two counting problems

- Given a group scheme $\mathbf{G} \leqslant \mathrm{GL}_n$, determine $|(\mathfrak{O}/\mathfrak{P}^k)^n/\mathbf{G}(\mathfrak{O}/\mathfrak{P}^k)|$.
- Given a group scheme $\mathbf{G}$, determine $\mathrm{k}(\mathbf{G}(\mathfrak{O}/\mathfrak{P}^k))$.

Questions

- What kinds of problems are these?
- How *"wild"* can they get?
- Why are these counting problems often *"tame"* for examples of interest?
- What does any of this have to do with tensors?

The Joy of... unipotent groups

Slogan I

Linear orbits and conjugacy classes of unipotent groups over quotients of compact DVRs are (generically) controlled by rank loci within spaces of matrices.

Slogan II

For the enumeration of linear orbits and conjugacy classes of unipotent groups in generic residue characteristic, we only need to consider groups of class at most 2.

These slogans draw upon work of Boston & Isaacs (2004), O'Brien & Voll (2015), R. (2018), and various "folklore" observations.

Ancient history:
Two perspectives on counting orbits

Let G act on X.

Cauchy-Frobenius/Burnside/Orbit-Counting Lemma:

$$\begin{aligned}|X/G| &= \frac{1}{|G|}\sum_{x\in X}|\mathrm{St}_G(x)| \\ &= \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_X(g)|.\end{aligned}$$

We can therefore count orbits...

- ... by partitioning X according to the orders of stabilisers, or
- ... by partitioning G according to sizes of fixed point sets.

Abelian groups from modules of matrices

Let R be a ring. For $a \in \mathrm{M}_{d\times e}(R)$, define

$$\hat{a} = \begin{bmatrix} 1_d & a \\ 0 & 1_e \end{bmatrix} \in \mathrm{GL}_{d+e}(R).$$

Let $M \subset \mathrm{M}_{d\times e}(R)$ be a submodule. The group $\hat{M}$ acts on R^{d+e} by right multiplication.

Lemma

Within the group $\hat{M}$:

- Fixed point sets $\longleftrightarrow$ kernels.
- Stabilisers $\longleftrightarrow$ annihilators.

In detail, let $(x, y) \in R^d \oplus R^e$ and $a \in M$. Then:

- $\mathrm{Fix}_{R^d \oplus R^e}(\hat{a}) = \mathrm{Ker}(a) \oplus R^e$.
- $\mathrm{St}_{\hat{M}}(x, y) = \widehat{\mathrm{Ann}_M(x)}$.

Linear orbits of unipotent groups

- Let $M \subset \mathrm{M}_{d\times e}(\mathbf{Z})$ be an isolated submodule.
- For each ring R, let $M(R) =$ image of $M \otimes R \to \mathrm{M}_{d\times e}(R)$.
- Let $\mathbf{G}_M(R) := \widehat{M(R)} = \begin{bmatrix} 1 & M(R) \\ 0 & 1 \end{bmatrix}$.

  Then $\mathbf{G}_M$ is a subgroup scheme of U_{d+e}.
- We can express $|\mathbf{F}_q^{d+e}/\mathbf{G}_M(\mathbf{F}_q)|$ in terms of the number of matrices of given rank in $M(\mathbf{F}_q)$. Those are numbers of $\mathbf{F}_q$-points of schemes over $\mathbf{Z}$.

Proposition

(R. 2018)

Given a unipotent group scheme $\mathbf{G} \leqslant \mathrm{U}_n$, there exists M such that $\mathbf{G}(\mathfrak{O}/\mathfrak{P}^k)$ and $\mathbf{G}_M(\mathfrak{O}/\mathfrak{P}^k)$ have essentially the same numbers of orbits on their natural modules... except possibly in small residue characteristic.

Class-2 groups from alternating products

Let $\diamond\colon \mathbf{Z}^d \times \mathbf{Z}^d \to \mathbf{Z}^e$ be an alternating bilinear map.

The **Baer group scheme** $\mathbf{G}_\diamond$ has the following properties:

- $\mathbf{G}_\diamond(R) = R^d \oplus R^e$ as sets for each ring R.
- $\Big[(x,y),(x',y')\Big] = (0, x \diamond_R x')$ for $x, x' \in R^d$ and $y, y' \in R^e$.

Lemma

$\mathrm{C}_{\mathbf{G}_\diamond(R)}(x,y) = \mathrm{Ker}(x \diamond_R \cdot) \oplus R^e.$

Proposition

("Folklore"; R. & Voll 2019^+)

Given a unipotent group scheme $\mathbf{G}$, there exists $\diamond$ such that $\mathbf{G}(\mathfrak{O}/\mathfrak{P}^k)$ and $\mathbf{G}_\diamond(\mathfrak{O}/\mathfrak{P}^k)$ have essentially the same class numbers... except possibly in small residue characteristic.

Enumerating matrices by rank is wild

Theorem

(Belkale & Brosnan 2003)

Counting invertible symmetric matrices with constrained support over $\mathbf{F}_q$ is as hard as counting $\mathbf{F}_q$-points on schemes (over $\mathbf{Z}$).

$\sum \text{wild} = \text{tame}\ldots\quad \text{sometimes}$

Example

(Carnevale & R. 2022)

Let

$$M = \Big\{[x_{ij}] \in \mathrm{M}_3(\mathbf{Z}) : x_{11} + x_{33} = x_{12} + x_{21} = x_{13} + x_{22} + x_{32} = x_{23} + x_{31} = 0\Big\}.$$

- 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 $\mathbf{F}_q$.

Remark

- The existence of arbitrarily wild examples of this form follows by combining Belkale & Brosnan (2003) and R. & Voll (2019^+).
- The roles of orbit and fixed point sizes can be interchanged.

Enter zeta functions

Definition

Let $\mathbf{G} \curvearrowright \mathbf{X}$ be an action of a group scheme $\mathbf{G}$ on a scheme $\mathbf{X}$ over a ring R. The **orbit-counting zeta function** of $\mathbf{G} \curvearrowright \mathbf{X}$ is

$$\zeta^{\mathrm{oc}}_{\mathbf{G} \curvearrowright \mathbf{X}}(s) = \sum_{I \triangleleft R} |\mathbf{X}(R/I)/\mathbf{G}(R/I)| \, |R/I|^{-s}.$$

Definition

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

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

In other words, this is the orbit-counting zeta function of $\mathbf{G}$ acting on itself by conjugation.

Remark

Several relatives and variants of these zeta functions have been studied in the literature:

- Du Sautoy (2004) introduced zeta functions enumerating conjugacy classes of congruence quotients of p-adic matrix groups. These were studied further by Berman et al. (2013), Lins (2019, 2020), R. (2018, 2020).
- Avni et al. (2016) investigated what they called *similarity class zeta functions*. These enumerate adjoint orbits of certain group schemes.

Example

(Berman et al. 2013, R. 2018)

$\zeta^{\mathrm{cc}}_{\mathrm{U}_3}(s) = \zeta(s-1)\zeta(s-2)/\zeta(s)$, where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function.

Lemma (Euler product)

Let $\mathcal{O}$ be the ring of integers of a global field K. Let $\mathbf{G} \curvearrowright \mathbf{X}$ over $\mathcal{O}$. Then:

$$\zeta^{\mathrm{oc}}_{\mathbf{G} \curvearrowright \mathbf{X}}(s) = \prod_{v \in \mathcal{V}_K} \zeta^{\mathrm{oc}}_{(\mathbf{G} \otimes \mathcal{O}_v) \curvearrowright (\mathbf{X} \otimes \mathcal{O}_v)}(s).$$

This is really just the Chinese remainder theorem!

By drawing upon well-known (but non-trivial!) results in the area, we obtain the following:

Theorem (rationality)

Let $\mathbf{G} \curvearrowright \mathbf{X}$ over a compact DVR $\mathfrak{O}$ of characteristic zero.

Then $\zeta^{\mathrm{oc}}_{\mathbf{G} \curvearrowright \mathbf{X}}(s) \in \mathbf{Q}(q^{-s})$, where q denotes the size of the residue field of $\mathfrak{O}$.

Theorem (geometric "Denef-formulae")

Let K be a number field with ring of integers $\mathcal{O}$. Let $\mathbf{G} \curvearrowright \mathbf{X}$ over $\mathcal{O}$. Then there are $\mathcal{O}$-schemes $V_1, \ldots, V_r$ and $W_1(X,T), \ldots, W_r(X,T) \in \mathbf{Q}(X,T)$ such that for almost all $v \in \mathcal{V}_K$,

$$\zeta^{\mathrm{cc}}_{\mathbf{G} \otimes \mathcal{O}_v}(s) = \frac{1}{\#\mathbf{G}(\mathfrak{K}_v)} \sum_{i=1}^{r} \#V_i(\mathfrak{K}_v) \cdot W_i(q_v, q_v^{-s}),$$

where $\mathfrak{K}_v =$ residue field of $\mathcal{O}_v$ of size q_v.

By drawing upon well-known (but non-trivial!) results in the area, we obtain the following:

Theorem (rationality)

Let $\mathbf{G} \curvearrowright \mathbf{X}$ over a compact DVR $\mathfrak{O}$ of characteristic zero.

Then $\zeta^{\mathrm{oc}}_{\mathbf{G} \curvearrowright \mathbf{X}}(s) \in \mathbf{Q}(q^{-s})$, where q denotes the size of the residue field of $\mathfrak{O}$.

Theorem (geometric "Denef-formulae")

Let K be a number field with ring of integers $\mathcal{O}$. Let $\mathbf{G} \curvearrowright \mathbf{X}$ over $\mathcal{O}$. Then there are $\mathcal{O}$-schemes $V_1, \dots, V_r$ and $W_1(X,T), \dots, W_r(X,T) \in \mathbf{Q}(X,T)$ such that for almost all $v \in \mathcal{V}_K$,

$$\zeta^{\mathrm{cc}}_{\mathbf{G} \otimes \mathcal{O}_v}(s) = \frac{1}{\#\mathbf{G}(\mathfrak{K}_v)} \sum_{i=1}^{r} \#V_i(\mathfrak{K}_v) \cdot W_i(q_v, q_v^{-s}),$$

where $\mathfrak{K}_v =$ residue field of $\mathcal{O}_v$ of size q_v.

Question

How *"wild"* can this actually get?

Average sizes of kernels

Definition

A **module representation** over a ring R is an R-linear map

$$\theta\colon M \to \mathrm{Hom}(V, W).$$

Equivalently, a module representation is an R-linear map

$$V \otimes M \to W.$$

Our motivating examples:

- Inclusions of submodules of $\mathrm{M}_{d\times e}(R)$.
- Adjoint representations of (Lie) algebras.

Definition

The <u>**a**</u>verage <u>**s**</u>ize of the <u>**k**</u>ernel associated with θ is

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

Definition

The **ask zeta function** associated with a module representation θ over a ring R is

$$\zeta_\theta^{\mathrm{ask}}(s) = \sum_{I \lhd R} \mathrm{ask}(\theta \otimes R/I)\,|R/I|^{-s}.$$

Theorem

(R. 2018)

Let $\mathbf{G} \leqslant \mathrm{U}_d$.

- Let $\mathfrak{g} \subset \mathfrak{n}_d(\mathbf{Z})$ be a $\mathbf{Z}$-form of the Lie algebra of $\mathbf{G}$. Then for each compact DVR $\mathfrak{O}$, we have $\zeta^{\mathrm{oc}}_{(\mathbf{G}\otimes\mathfrak{O})\curvearrowright(\mathbf{A}^d\otimes\mathfrak{O})}(s) = \zeta^{\mathrm{ask}}_{\mathfrak{g}\otimes\mathfrak{O}}(s)$... except possibly in small residue characteristic.
- $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathfrak{O}}(s) = \zeta^{\mathrm{ask}}_{\mathrm{ad}_{\mathfrak{g}}\otimes\mathfrak{O}}(s)$ for each compact DVR $\mathfrak{O}$... except possibly in small residue characteristic.

Definition

The **ask zeta function** associated with a module representation θ over a ring R is

$$\zeta_{\theta}^{\mathrm{ask}}(s) = \sum_{I \triangleleft R} \mathrm{ask}(\theta \otimes R/I)\,|R/I|^{-s}.$$

Theorem

(R. 2018)

Let $\mathbf{G} \leqslant \mathrm{U}_d$.

- Let $\mathfrak{g} \subset$ ch compact DVR $\mathfrak{O}$, ly in small residue characteristic.

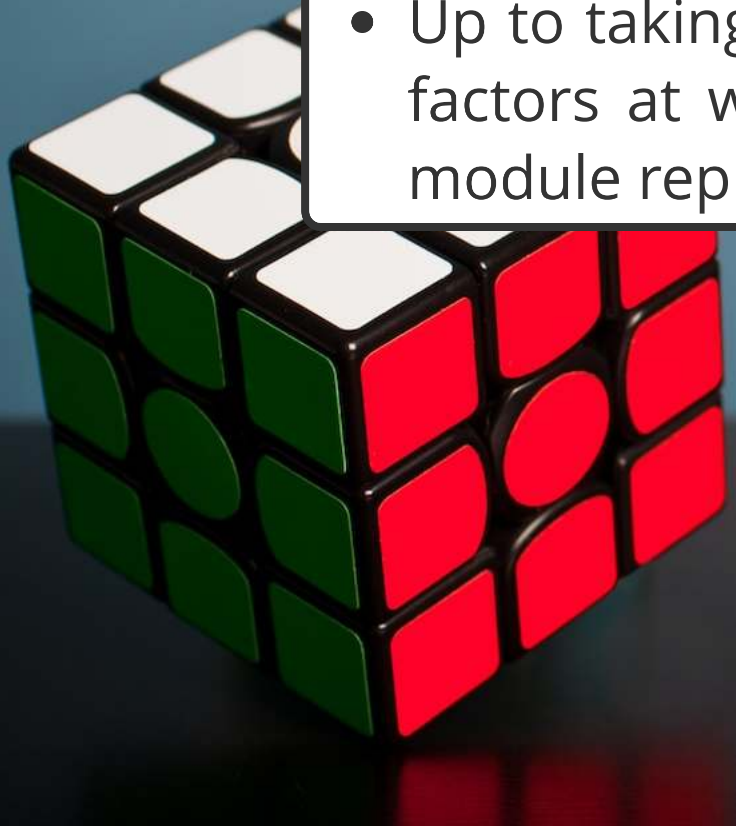
$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| \rightsquigarrow \frac{1}{|\mathfrak{g}|}\sum_{a\in\mathfrak{g}}|\mathrm{Ker}(a)|$$

- $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathfrak{O}}(s) = \zeta^{\mathrm{ask}}_{\mathrm{ad}_{\mathfrak{g}}\otimes\mathfrak{O}}(s)$ for each compact DVR $\mathfrak{O}$… except possibly in small residue characteristic.

Why pass to ask zeta functions?

- We saw: class-counting and {linear orbit}-counting zeta functions of unipotent groups are essentially examples of ask zeta functions.
- Conversely, ask zeta functions enumerate orbits of suitable groups.
- Ask zeta functions can be studied using a combination of tools from algebra, combinatorics, geometry, logic, and p-adic integration.
- In contrast to many other zeta functions in asymptotic group theory, ask zeta functions are quite well-behaved w.r.t. algebraic operations. In particular: *duality functors* for module representations.

Knuth duality



- Under suitable assumptions, a module representation $\theta\colon M \to \mathrm{Hom}(V, W)$ is the same as an element of $M^* \otimes V^* \otimes W$.
- Up to taking duals, we can shuffle the tensor factors at will. We thus obtain a total of six module representations derived from one.

Theorem

(R. 2020)

Let θ' be a Knuth dual of θ. Then

$$\zeta^{\mathrm{ask}}_{\theta'}(s) \sim \zeta^{\mathrm{ask}}_{\theta}(s).$$

Hiding in plain sight: constant rank spaces

- Let F be a field. Consider matrix-vector multiplication
$$F^d \otimes \mathrm{M}_{d\times e}(F) \to F^e.$$
- We can partition $\mathrm{M}_{d\times e}(F)$ according to the ranks of the associated maps $F^d \to F^e$.
- It's *much* easier to swap tensor factors and partition F^d according to the ranks of the maps $\mathrm{M}_{d\times e}(F) \to F^e$.
- Indeed, the nonzero maps of this form all have rank e! We're looking at a **constant rank space.**

These observations lie at the heart of the following:

Proposition

(R. 2018)

Let $\mathfrak{O}$ be a compact DVR with residue field of size q.

Then
$$\zeta^{\mathrm{ask}}_{\mathrm{M}_{d\times e}(\mathfrak{O})}(s) = \frac{1-q^{-e-s}}{(1-q^{-s})(1-q^{d-e-s})}$$

Computing ask zeta functions

Definition

Let $X = (X_1, \ldots, X_n)$ and let $M(X)$ be an $\mathfrak{O}[X]$-module. Define

$$\zeta_{M(X)}(s) := \int_{\mathfrak{O}^n \times \mathfrak{O}} \#(M(x) \otimes \mathfrak{O}/y) \cdot |y|^s \,\mathrm{d}\mu(x, y).$$

Proposition

(R. & Voll 2019^+)

Let $\theta \colon M \to \mathrm{Hom}(V, W)$ be a module representation over $\mathfrak{O}$. Suppose that all modules in sight are free of finite rank.

Let $A(X)$ be a matrix of linear forms representing θ.

Then

$$\zeta_\theta^{\mathrm{ask}}(s) \sim \zeta_{\mathrm{Coker}\, A(X)}(s).$$

Definition

Let $X = (X_1, \dots, X_n)$ and let $M(X)$ be an $\mathfrak{O}[X]$-module. Define

$$\zeta_{M(X)}(s) := \int_{\mathfrak{O}^n \times \mathfrak{O}} \#(M(x) \otimes \mathfrak{O}/y) \cdot |y|^s \, \mathrm{d}\mu(x, y).$$

Rewriting $\zeta_{M(X)}(s)$: minors

Definition

Let $M \approx \operatorname{Coker} A$ be an R-module, where $A \in \mathrm{M}_{m \times n}(R)$.

The ith **Fitting ideal** $\mathrm{Fit}_i(M)$ is generated by $(n-i) \times (n-i)$ minors of A.

Proposition

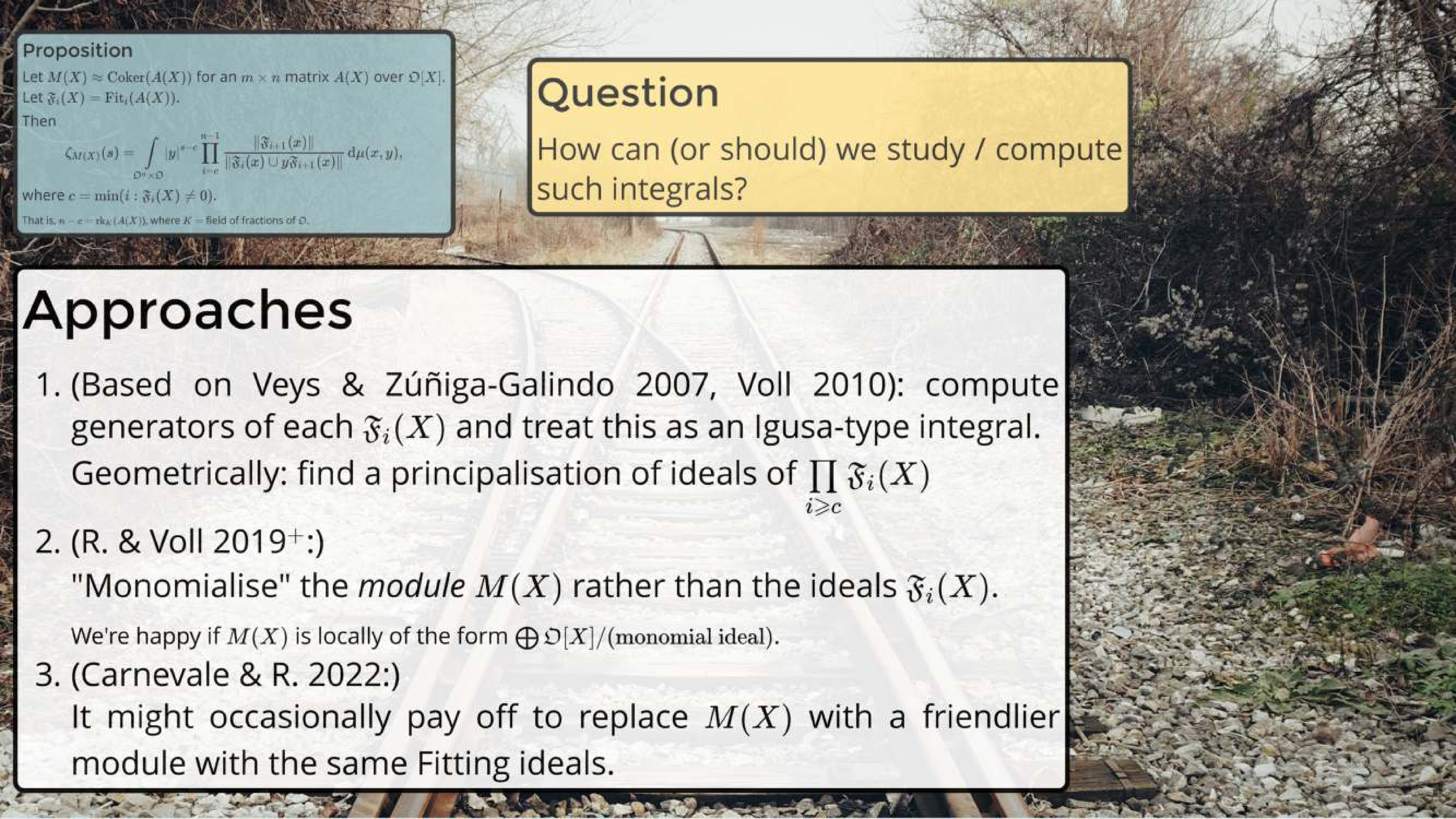
Let $M(X) \approx \operatorname{Coker} A(X)$ for an $m \times n$ matrix $A(X)$ over $\mathfrak{O}[X]$.
Let $\mathfrak{F}_i(X) = \mathrm{Fit}_i(A(X))$.

Then

$$\zeta_{M(X)}(s) = \int_{\mathfrak{O}^n \times \mathfrak{O}} |y|^{s-c} \prod_{i=c}^{n-1} \frac{\|\mathfrak{F}_{i+1}(x)\|}{\|\mathfrak{F}_i(x) \cup y\mathfrak{F}_{i+1}(x)\|} \, \mathrm{d}\mu(x, y),$$

where $c = \min(i : \mathfrak{F}_i(X) \neq 0)$.

That is, $n - c = \mathrm{rk}_K(A(X))$, where K = field of fractions of $\mathfrak{O}$.



Proposition

Let $M(X) \approx \operatorname{Coker}(A(X))$ for an $m \times n$ matrix $A(X)$ over $\mathfrak{O}[X]$.
Let $\mathfrak{F}_i(X) = \operatorname{Fit}_i(A(X))$.
Then

$$\zeta_{M(X)}(s) = \int_{\mathfrak{O}^n \times \mathfrak{O}} |y|^{s-c} \prod_{i=c}^{n-1} \frac{\|\mathfrak{F}_{i+1}(x)\|}{\|\mathfrak{F}_i(x) \cup y\mathfrak{F}_{i+1}(x)\|} \,\mathrm{d}\mu(x,y),$$

where $c = \min(i : \mathfrak{F}_i(X) \neq 0)$.

That is, $n - c = \operatorname{rk}_K(A(X))$, where $K =$ field of fractions of $\mathfrak{O}$.

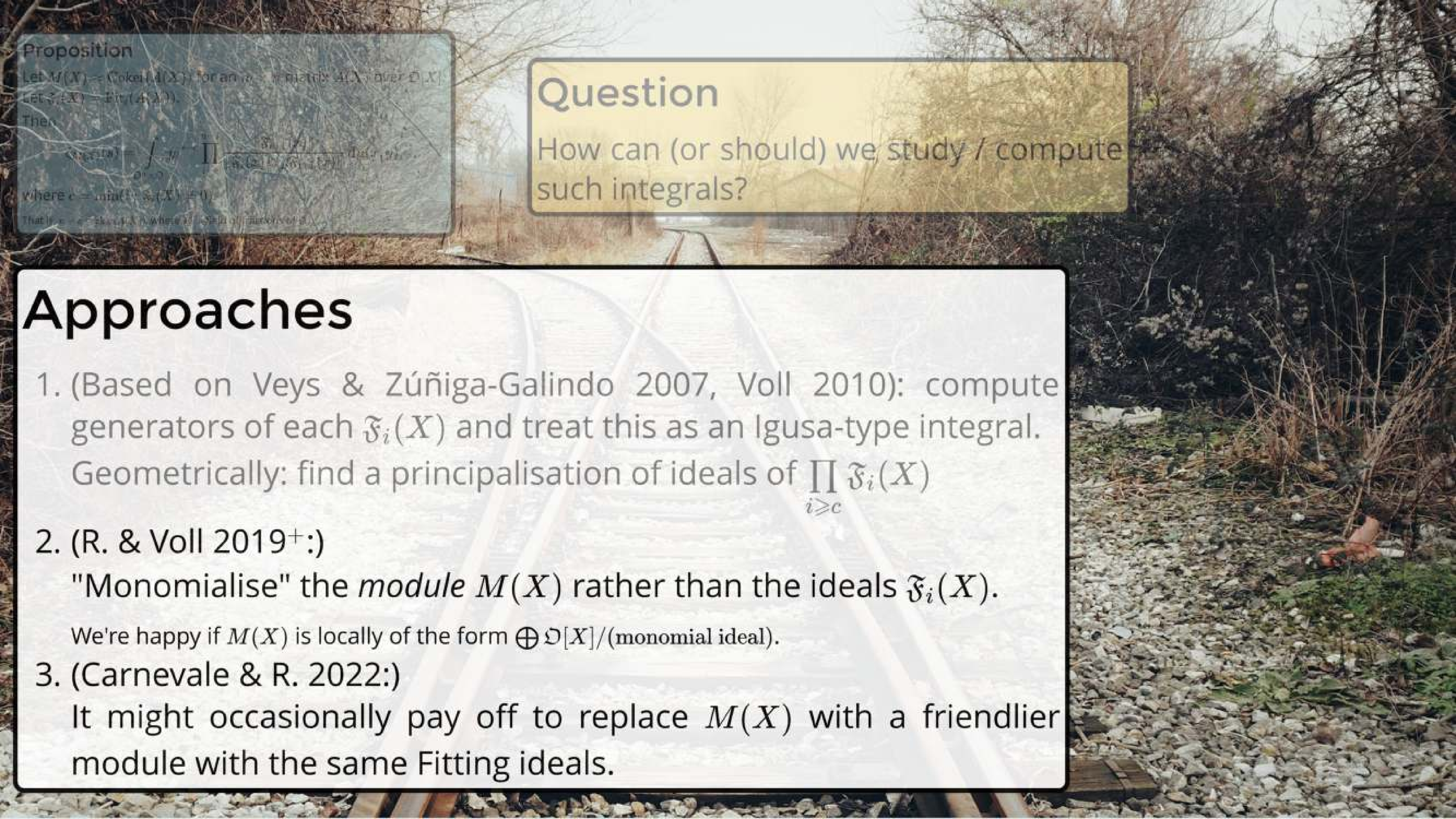
Question

How can (or should) we study / compute such integrals?

Approaches

1. (Based on Veys & Zúñiga-Galindo 2007, Voll 2010): compute generators of each $\mathfrak{F}_i(X)$ and treat this as an Igusa-type integral. Geometrically: find a principalisation of ideals of $\prod_{i \geqslant c} \mathfrak{F}_i(X)$
2. (R. & Voll 2019$^+$:) "Monomialise" the *module* $M(X)$ rather than the ideals $\mathfrak{F}_i(X)$.

   We're happy if $M(X)$ is locally of the form $\bigoplus \mathfrak{O}[X]/(\text{monomial ideal})$.
3. (Carnevale & R. 2022:) It might occasionally pay off to replace $M(X)$ with a friendlier module with the same Fitting ideals.



Proposition

Let $M(X) = \mathrm{Coker}(A(X))$ for an [illegible] matrix $A(X)$ over $\mathfrak{O}[X]$.
Let $\mathfrak{F}_i(X) = \mathrm{Fit}_i(A(X))$.
Then

[illegible]

where $c = \min(i : \mathfrak{F}_i(X) \neq 0)$.

That is [illegible]

Question

How can (or should) we study / compute such integrals?

Approaches

1. (Based on Veys & Zúñiga-Galindo 2007, Voll 2010): compute generators of each $\mathfrak{F}_i(X)$ and treat this as an Igusa-type integral. Geometrically: find a principalisation of ideals of $\prod_{i \geqslant c} \mathfrak{F}_i(X)$
2. (R. & Voll 2019^+:) "Monomialise" the *module* $M(X)$ rather than the ideals $\mathfrak{F}_i(X)$.
   We're happy if $M(X)$ is locally of the form $\bigoplus \mathfrak{O}[X]/(\text{monomial ideal})$.
3. (Carnevale & R. 2022:) It might occasionally pay off to replace $M(X)$ with a friendlier module with the same Fitting ideals.

Free nilpotent groups

- Let $\mathsf{F}_{c,d}$ be the group scheme associated with the free nilpotent Lie algebra of class c and rank d.
- Example: $\mathsf{F}_{2,2} = \mathrm{U}_3$
- O'Brien & Voll (2015) explicitly determined the number of conjugacy classes of given size of $\mathsf{F}_{c,d}(\mathbf{F}_q)$ in terms of Witt's dimension formula.

Question

What are the (local) class-counting zeta functions associated with $\mathsf{F}_{c,d}$?

Write $t = q^{-s}$.

Theorem

(Lins 2020)

For each compact DVR $\mathfrak{O}$ with residue field size q,

$$\zeta^{\mathrm{cc}}_{\mathsf{F}_{2,d}\otimes\mathfrak{O}}(s) = \frac{1 - q^{\binom{d-1}{2}}t}{\left(1 - q^{\binom{d}{2}}t\right)\left(1 - q^{\binom{d}{2}+1}t\right)}.$$

Two further proofs are known at this point.

Theorem

(Carnevale & R. 2022)

For each compact DVR $\mathfrak{O}$ with residue field size q and $\gcd(q,6) = 1$,

$$\zeta^{\mathrm{cc}}_{\mathsf{F}_{3,d}\otimes\mathfrak{O}}(s) = \frac{\left(1 - q^{\frac{(d-1)(d^2+d-3)}{3}}t\right)\left(1 - q^{\frac{(d-2)d(d+2)}{3}}t\right)}{\left(1 - q^{\frac{(d-1)d(d+1)}{3}}t\right)\left(1 - q^{\frac{d^3-d+3}{3}}t\right)\left(1 - q^{\frac{(2d^2+3d-11)d}{6}}t\right)}.$$

Write $t = q^{-s}$.

Theorem

(Lins 2020)

For each compact DVR $\mathfrak{O}$ with residue field size q,

$$\zeta^{\mathrm{cc}}_{\mathsf{F}_{2,d}\otimes\mathfrak{O}}(s) = \frac{1 - q^{\binom{d-1}{2}}t}{\left(1 - q^{\binom{d}{2}}t\right)\left(1 - q^{\binom{d}{2}+1}t\right)}.$$

Reason: another constant rank space!

Two further proofs are known at this point.

Theorem

(Carnevale & R. 2022)

For each compact DVR $\mathfrak{O}$ with residue field size q and $\gcd(q,6) = 1$,

$$\zeta^{\mathrm{cc}}_{\mathsf{F}_{3,d}\otimes\mathfrak{O}}(s) = \frac{\left(1 - q^{\frac{(d-1)(d^2+d-3)}{3}}t\right)\left(1 - q^{\frac{(d-2)d(d+2)}{3}}t\right)}{\left(1 - q^{\frac{(d-1)d(d+1)}{3}}t\right)\left(1 - q^{\frac{d^3-d+3}{3}}t\right)\left(1 - q^{\frac{(2d^2+3d-11)d}{6}}t\right)}.$$

Theorem

(Carnevale & R. 2022)

For each compact DVR $\mathfrak{O}$ with residue field size q and $\gcd(q,6)=1$,

$$\zeta^{\mathrm{cc}}_{\mathsf{F}_{3,d}\otimes\mathfrak{O}}(s) = \frac{\left(1-q^{\frac{(d-1)(d^2+d-3)}{3}}t\right)\left(1-q^{\frac{(d-2)d(d+2)}{3}}t\right)}{\left(1-q^{\frac{(d-1)d(d+1)}{3}}t\right)\left(1-q^{\frac{d^2-d+2}{2}}t\right)\left(1-q^{\frac{(2d^2+3d-11)d}{6}}t\right)}.$$

Sketch of proof.

- Let $\mathfrak{a}_{c,d}$ be the free algebra generated by d symbols subject to the relations $x^2=0$ and
$$x_1(x_2(\dots(x_c x_{c+1})\dots))=0.$$
- 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. of $\mathfrak{f}_{c,d}$).
- By earlier theorems, $\zeta^{\mathrm{cc}}_{\mathsf{F}_{c,d}\otimes\mathfrak{O}}(s)=\zeta^{\mathrm{ask}}_{\hat{\alpha}_{c,d}\otimes\mathfrak{O}}(s)$.
- Induction and a Gröbner basis calculation (using Macaulay2 or SageMath): for $c=3$, the two associated modules have the same Fitting ideals. Hence, $\zeta^{\mathrm{cc}}_{\mathsf{F}_{c,d}\otimes\mathfrak{O}}(s)=\zeta^{\mathrm{ask}}_{\alpha_{c,d}\otimes\mathfrak{O}}(s)$.
- The latter zeta functions turns out to (essentially) coincide with the class-counting zeta function of certain *graphical group schemes* attached to *threshold graphs* in the sense of (R. & Voll 2019^{+}). We can then read off our formula. ♦

Graphical groups

Definition

Let Γ be a graph with distinct vertices $v_1, \ldots, v_n$.

For a ring R, the **graphical group $\mathbf{G}_\Gamma(R)$** is defined as follows:

Generators: $x_1(r), \ldots, x_n(r)$ and $z_{ij}(r)$ for $i < j$ and $v_i \sim v_j$

Relations:

- $x_i(r)x_i(r') = x_i(r + r')$ and $z_{ij}(r)z_{ij}(r') = z_{ij}(r + r')$.
- For $i < j$,
  $$[x_i(r), x_j(r')] = \begin{cases} z_{ij}(rr'), & \text{if } v_i \sim v_j, \\ 1, & \text{otherwise.} \end{cases}$$
- Commutators are central.

Proposition

$\mathbf{G}_\Gamma$ represents a unipotent group scheme.

Example

- $\mathbf{G}_{\mathrm{K}_n} = \mathsf{F}_{2,n}$.
- $\mathbf{G}_{\mathrm{P}_n}(R)$ is the maximal quotient of class at most 2 of $\mathrm{U}_{n+1}(R)$.

Remark

$\mathbf{G}_\Gamma(\mathbf{Z})$ is the maximal quotient of class at most 2 of the right-angled Artin group

$$\left\langle x_1, \ldots, x_n \mid [x_i, x_j] = 1 \text{ whenever } v_i \not\sim v_j \right\rangle.$$

Question

How do class-counting zeta functions of graphical group schemes look like?

- These zeta functions can be expressed in terms of the rank loci of generic antisymmetric matrices with support constraints.
- This motivated R. & Voll (2019^+) 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)?

Uniformity Theorem

(R. & Voll 2019$^+$)

For each graph Γ, there exists $W_\Gamma(X,T) \in \mathbf{Q}(X,T) \cap \mathbf{Q}[X][\![T]\!]$ such that for each compact discrete valuation ring $\mathfrak{O}$,

$$\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma \otimes \mathfrak{O}}(s) = W_\Gamma(q, q^{-s}),$$

where q is the residue field size of $\mathfrak{O}$.

Remark

Our proof is constructive and gives rise to a practical algorithm, at least for graphs on very few vertices.

Implemented in Zeta.

skip

The Uniformity Theorem: under the hood

Lemma

(R. & Voll 2019^{+})

Let $M(X)$ be a **combinatorial** $\mathbf{Z}[X]$-module in the sense that

$$M(X) = \mathbf{Z}[X]/I_1 \oplus \cdots \oplus \mathbf{Z}[X]/I_\ell$$

for monomial ideals $I_1, \ldots, I_\ell$.

Then there exists $W(X,T) \in \mathbf{Q}(X,T)$ s.t.

$$\zeta_{M(X)\otimes\mathfrak{O}[X]}(s) = W(q, q^{-s})$$

for each compact DVR $\mathfrak{O}$ with residue field size q.

Adjacency modules

Definition

Let Γ be a graph with vertices $1, \ldots, n$. Write $X = (X_1, \ldots, X_n)$.

The **adjacency module** of Γ is

$$\mathrm{Adj}(\Gamma) = \frac{\mathbf{Z}[X]^n}{\langle X_i \mathrm{e}_j - X_j \mathrm{e}_i : i \sim j \text{ in } \Gamma \rangle}.$$

Proposition

(R. & Voll 2019^{+})

$\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma \otimes \mathfrak{O}}(s) \sim \zeta_{\mathrm{Adj}(\Gamma) \otimes \mathfrak{O}[X]}(s)$

Toric geometry to the rescue

Definition

Let $\sigma \subset \mathbf{R}^n_{\geqslant 0}$ be a cone.

- The **dual** of σ is $\sigma^* = \{\omega \in \mathbf{R}^n : \alpha \cdot \omega \geqslant 0 \text{ for all } \alpha \in \sigma\}$.
- The **toric ring** associated with σ is
$$\mathbf{Z}_\sigma = \mathbf{Z}[X^\omega : \omega \in \sigma^* \cap \mathbf{Z}^n] \supset \mathbf{Z}[X].$$

The Uniformity Theorem is a consequence of the following.

Theorem

(R. & Voll 2019$^+$)

Given Γ, there exists a fan $\mathcal{F}$ with support $\bigcup \mathcal{F} = \mathbf{R}^n_{\geqslant 0}$ such that $\mathrm{Adj}(\Gamma) \otimes \mathbf{Z}_\sigma$ is combinatorial for each $\sigma \in \mathcal{F}$.

skip

An illustration

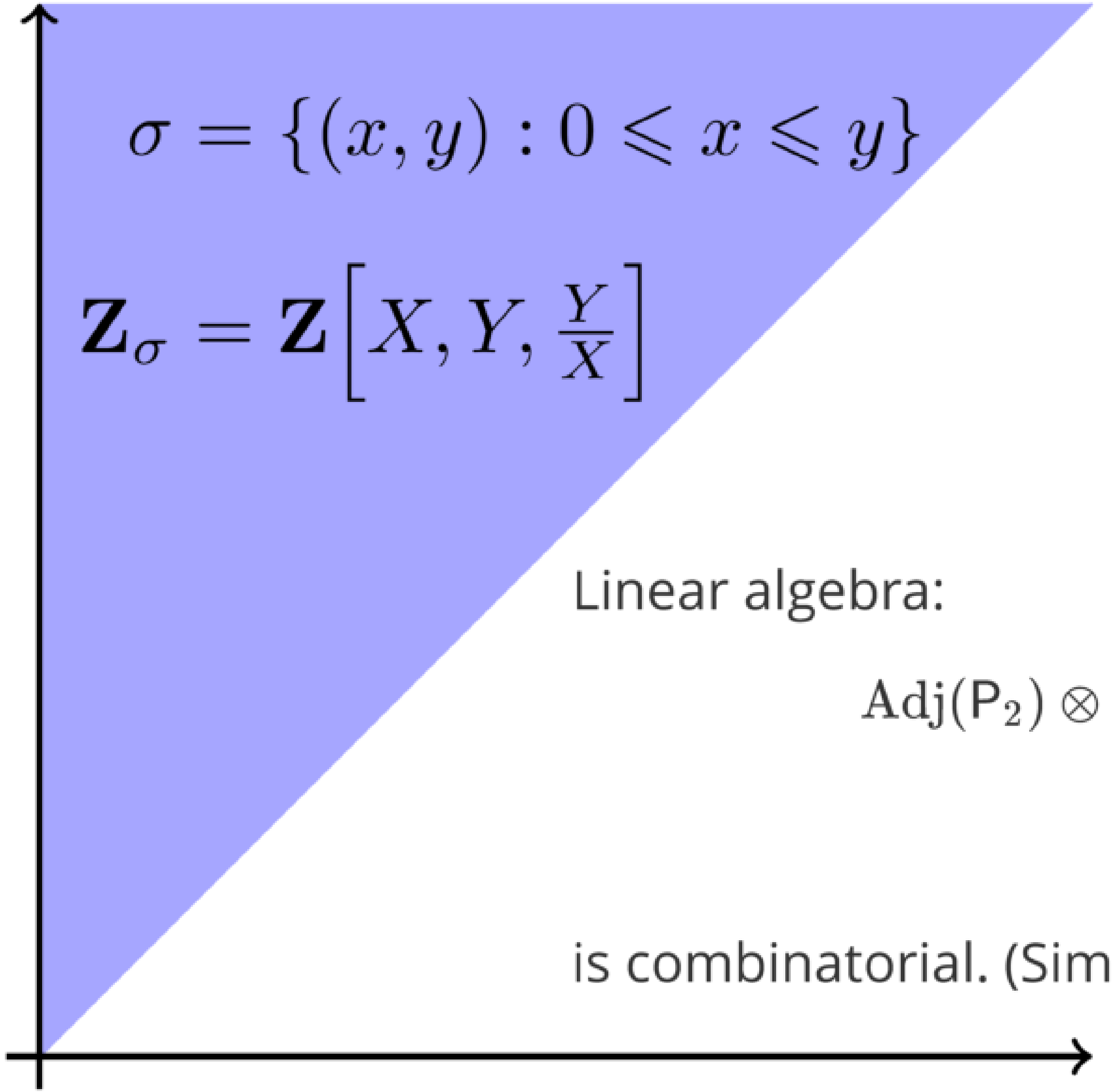
Let $\mathsf{P}_2 =$ 

Then

$$\mathrm{Adj}(\mathsf{P}_2) = \frac{\mathbf{Z}[X,Y]^2}{\langle(-Y,X)\rangle}.$$

Exercise. This module is not combinatorial.

However, it is "torically combinatorial"!



$$\sigma = \{(x,y) : 0 \leqslant x \leqslant y\}$$

$$\mathbf{Z}_\sigma = \mathbf{Z}\left[X, Y, \frac{Y}{X}\right]$$

Linear algebra:

$$\begin{aligned} \mathrm{Adj}(\mathsf{P}_2) \otimes \mathbf{Z}_\sigma &= \frac{\mathbf{Z}_\sigma^2}{\langle(-Y, X)\rangle} \\ &\approx \frac{\mathbf{Z}_\sigma}{\langle X \rangle} \oplus \mathbf{Z}_\sigma \end{aligned}$$

is combinatorial. (Similarly on the other side.)

Summary

- In many cases of interest, there are (more or less) algebraic reasons for the absence of geometry ("uniformity") from zeta functions counting orbits.
- The obvious notion of isomorphism (for modules or module representations) isn't quite right here. Fitting equivalence can be better, but there are downsides...
- Duality phenomena can foil attempts at trapping wild geometry within a counting problem.

Approximately wild things

Theorem

(R. 2022^{+})

Let Y be a scheme of finite type over $\mathbf{Z}$. Let $n \geqslant 1$.

Then there are finitely many

- commutative group schemes $\mathbf{M}_1, \ldots, \mathbf{M}_r \leqslant \mathrm{U}_{d_i}$,
- Baer group schemes $\mathbf{G}_1, \ldots, \mathbf{G}_r$, and
- Laurent polynomials $f_1(X), \ldots, f_r(X), g_1(X), \ldots, g_r(X) \in \mathbf{Z}[X^{\pm 1}]$

such that for each prime power q, the quantities

- $F(q) := \sum_{i=1}^{r} f_i(q)\mathrm{k}(\mathbf{G}_i(\mathbf{F}_q))$ and
- $G(q) := \sum_{i=1}^{r} g_i(q)\#(\mathbf{F}_q^{d_i}/\mathbf{M}_i(\mathbf{F}_q))$

are both integers which satisfy

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

Sketch of proof.

1. Let $M \subset \mathrm{M}_{d\times e}(\mathbf{F}_q)$ be a subspace of dimension ℓ. Let $V_i = \{a \in M : \mathrm{rk}(a) = i\}$. Then
$$\mathrm{ask}(M) = \sum_{i=0}^{d} \#V_i \cdot q^{d-i-\ell}.$$
2. Let ${}^{m}M := \{\mathrm{diag}(a, \ldots, a) : a \in M\}$. Write $q = p^e$. Then
$$\lim_{m\to\infty} \mathrm{ask}({}^{m}M) = q^{-\ell}\#V_d$$
in $\mathbf{Q}_p$.
3. Using the work of Belkale and Brosnan (2003), we know that the $\#V_d$ can be arbitrarily wild.
4. By combining the previous points, we can produce modules of matrices over $\mathbf{Z}$ whose average sizes of kernels over $\mathbf{F}_q$ are wild modulo q^n, uniformly in q.
5. Using techniques discussed before (Baer group schemes, etc.), we can manufacture group schemes around such modules. ◆

Where do we go from here?

Question

What is the scope of these methods for proving tameness / wildness of counting problems?

Thank you!