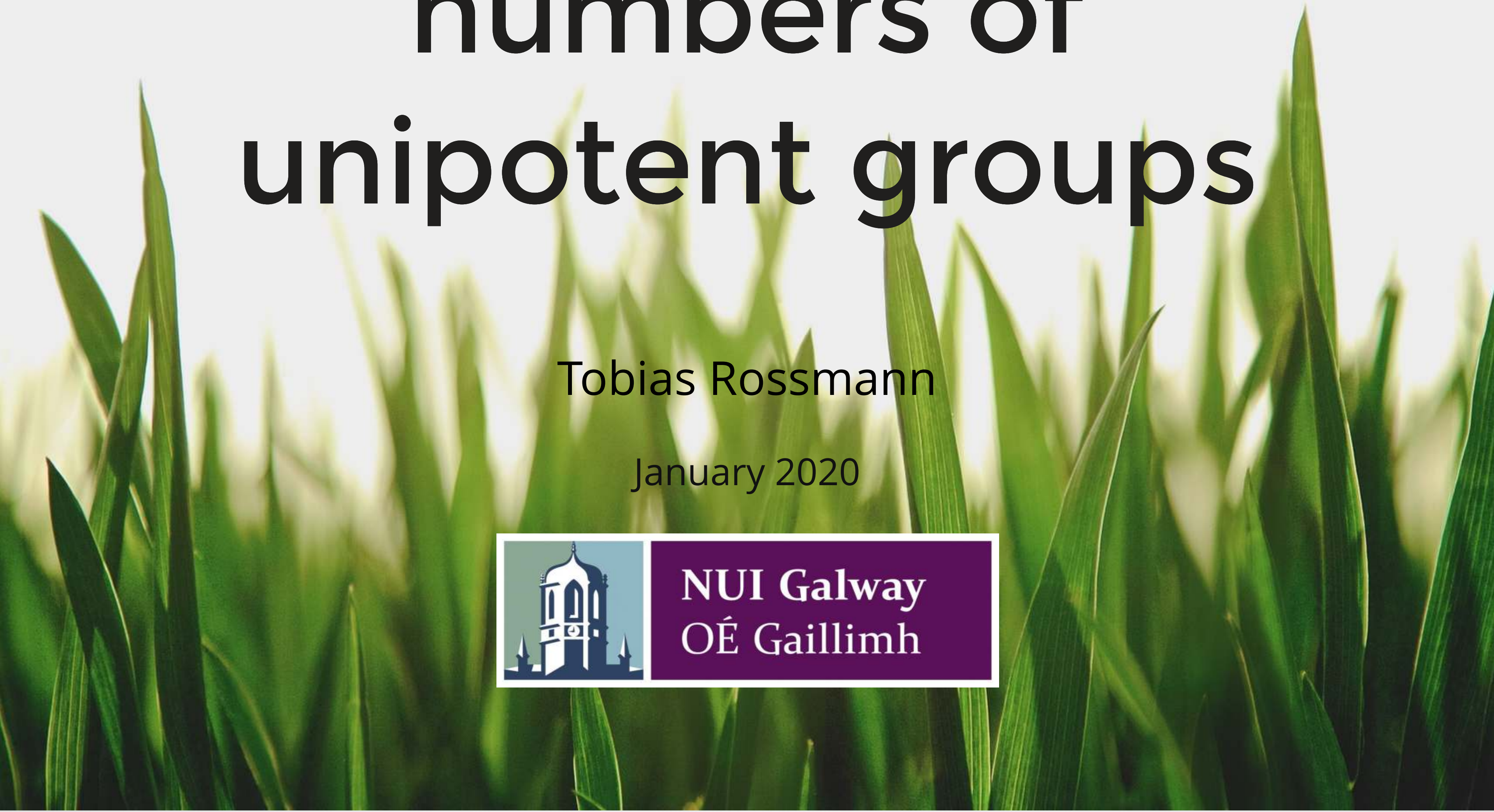
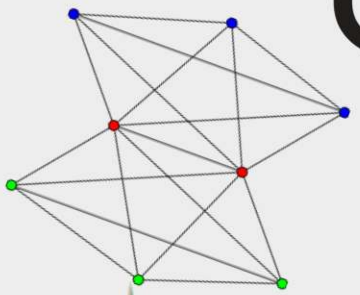
Growth of class numbers of unipotent groups



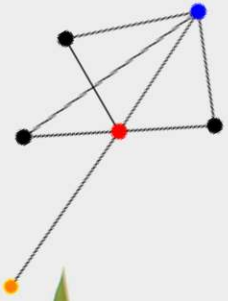
Tobias Rossmann

January 2020

NUI Galway
OÉ Gaillimh



Growth of class numbers of ~~unipotent~~ *graphical* groups



Tobias Rossmann

January 2020

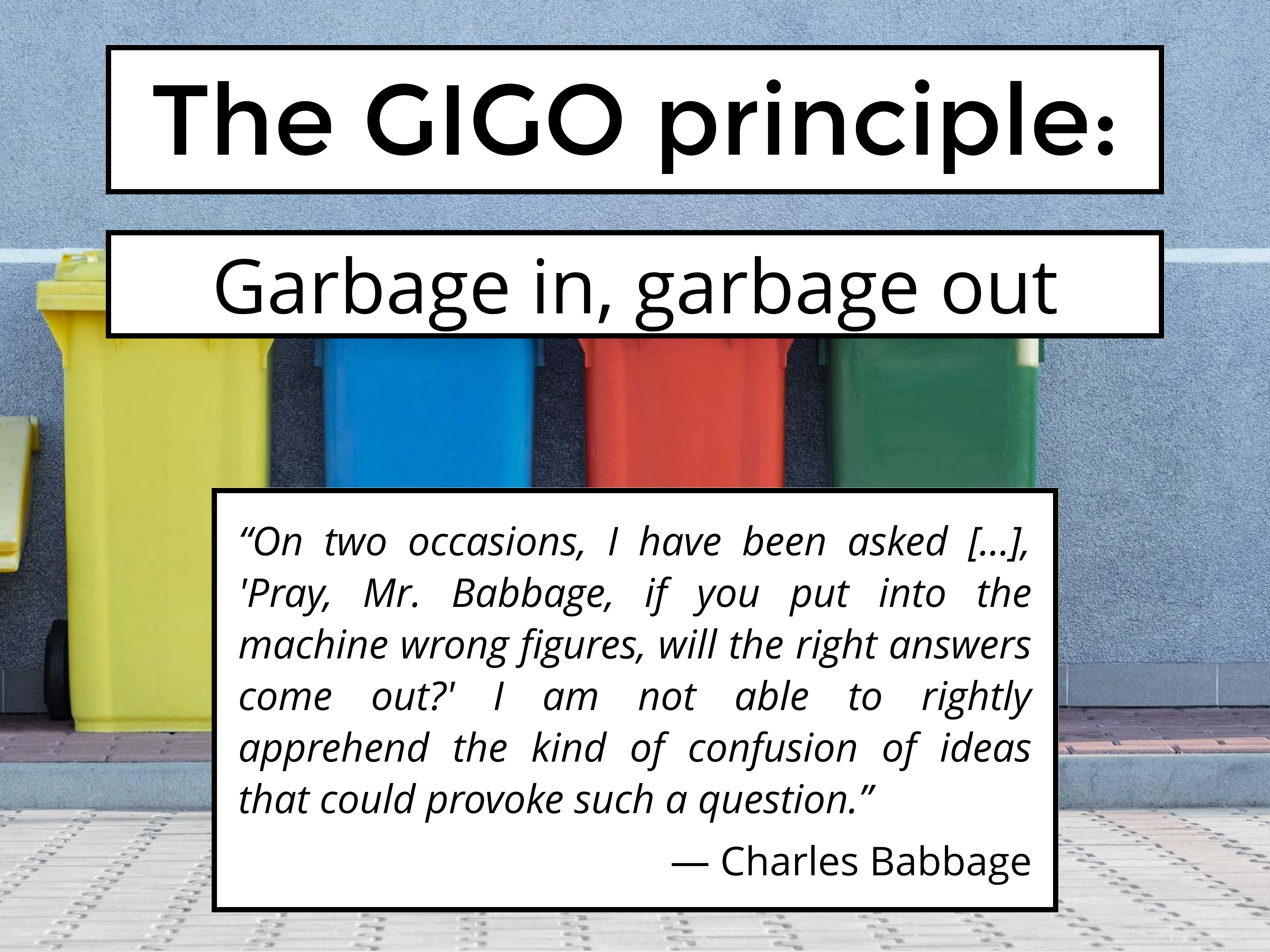
NUI Galway
OÉ Gaillimh

Ingredients…

- Enumeration of matrices
- Graphical groups
- Class counting zeta functions
- Toric geometry

...and where to find them

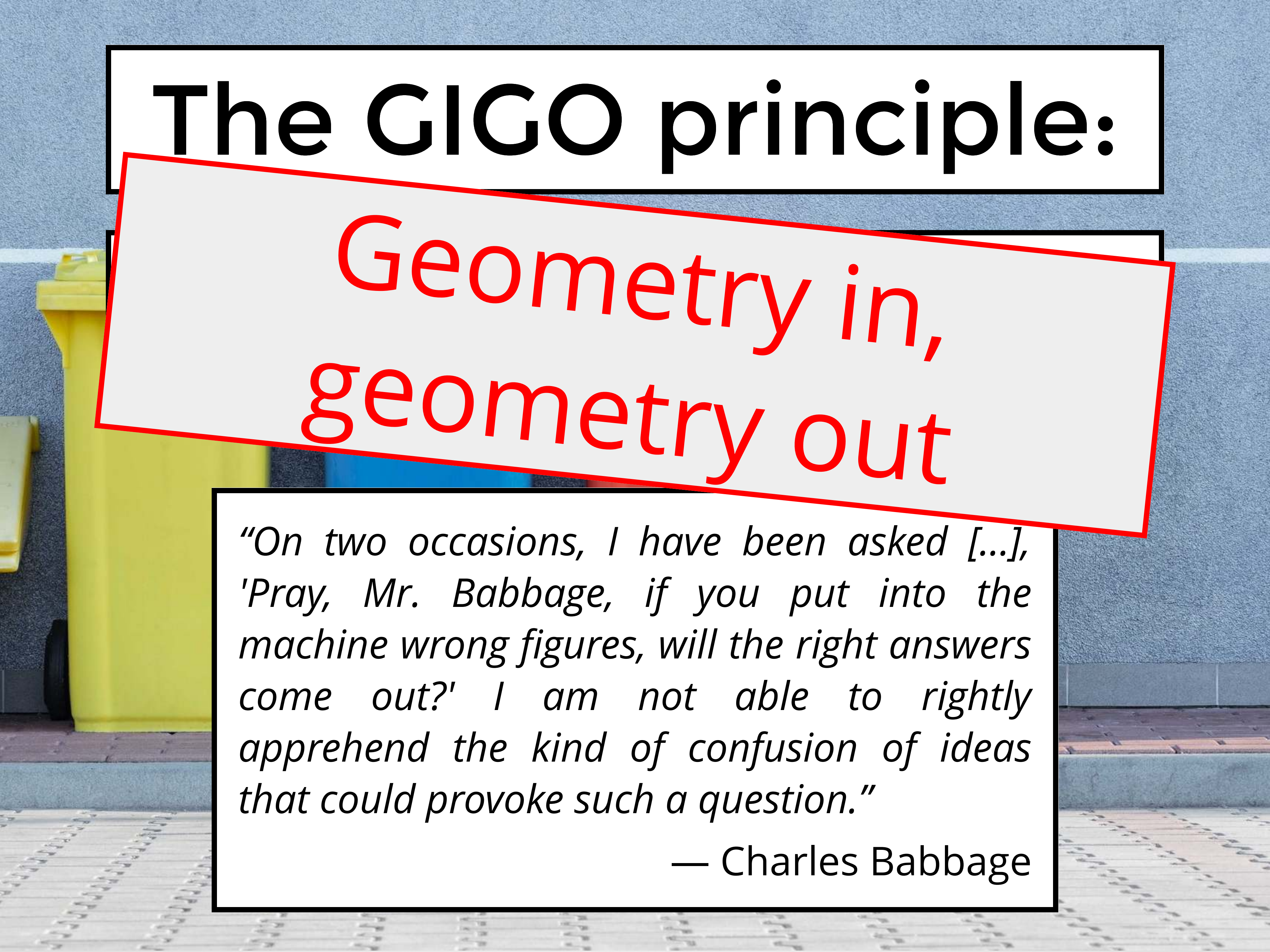
- R.: T*he average size of the kernel of a matrix and orbits of linear groups*, 2018.
- R.: *The average size of the kernel of a matrix and orbits of linear groups, II: duality*, 2020.
- R. & Voll: *Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints* (preprint), 2019. arXiv:1908.09589



The GIGO principle:

Garbage in, garbage out

> *“On two occasions, I have been asked […], 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' I am not able to rightly apprehend the kind of confusion of ideas that could provoke such a question.”*
>
> — Charles Babbage



The GIGO principle:

Geometry in, geometry out

> *“On two occasions, I have been asked […], 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' I am not able to rightly apprehend the kind of confusion of ideas that could provoke such a question.”*
>
> — Charles Babbage

Counting matrices by rank

Example

Let X be a $\mathbf{Z}$-defined space of matrices.

Let $X(\mathbf{F}_q)$ be the corresponding space of matrices over $\mathbf{F}_q$.

Then the number of matrices in $X(\mathbf{F}_q)$ of given rank r "depends geometrically" on q.

Sketch of proof. Let $A_1, \ldots, A_\ell$ be a basis of X. Then

$$x_1A_1 + \cdots + x_\ell A_\ell$$

has rank $< r$ iff all $r \times r$ minors of $x_1A_1 + \cdots + x_\ell A_\ell$ vanish.

Corollary

Linear algebra + rank constraints $\subset$ algebraic geometry.

Questions

- How much of algebraic geometry do we get?
- What happens for nice spaces of matrices?
- What does this have to do with group theory?

Counting matrices by rank: polynomiality

Theorem

(Landsberg 1893, Carlitz 1954, MacWilliams 1969, Buckhiester 1972, Bender 1974)

The following types of matrices of a given shape and given rank over $\mathbf{F}_q$ are given by polynomials in q:

- general rectangular,
- antisymmetric,
- symmetric, and
- traceless.

Theorem

(Lewis et al. 2011, Klein et al. 2014)

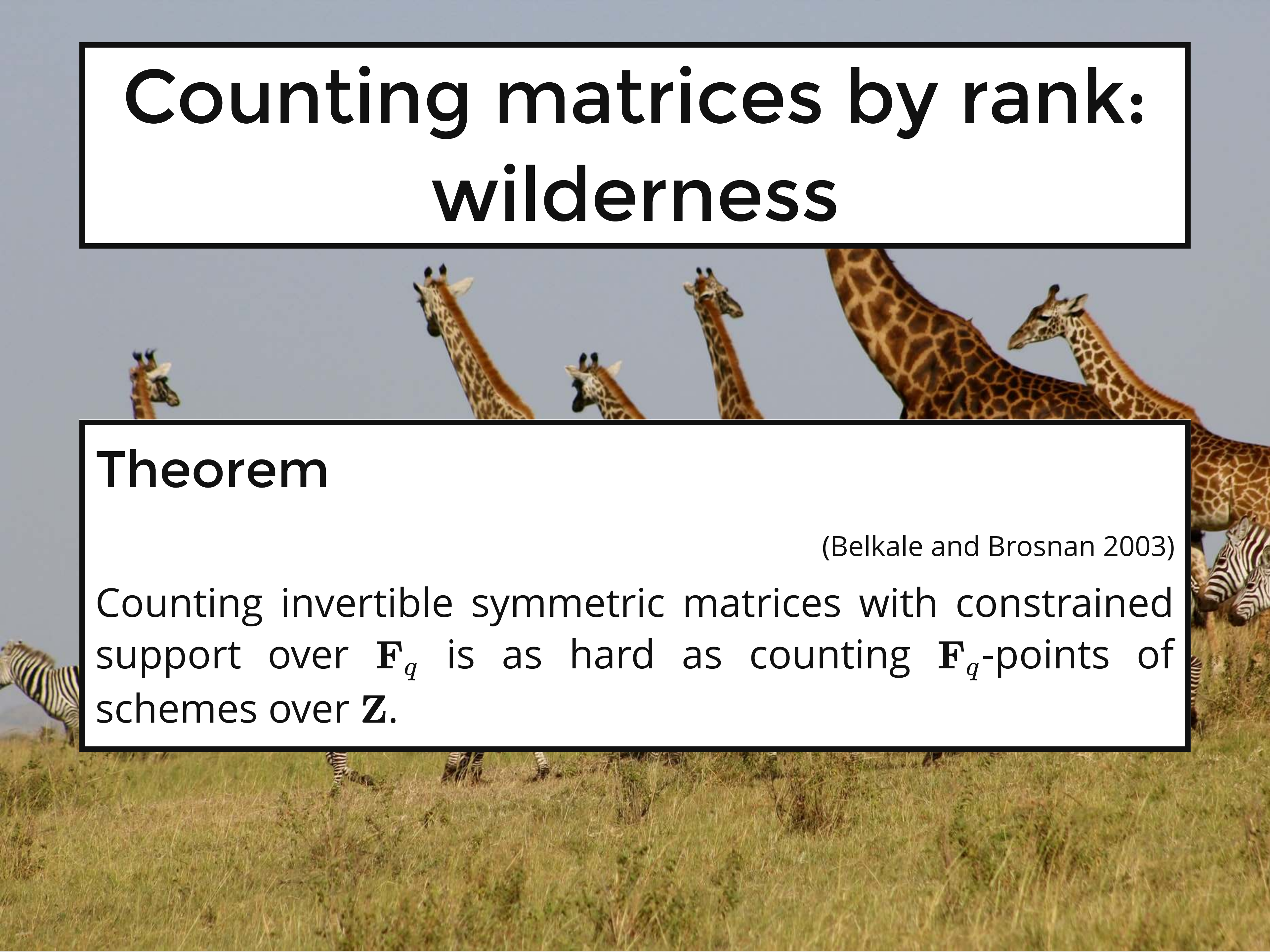
Similar polynomiality results, where entries in suitable positions are required to be zero.

Theorem

(Stembridge 1998)

Mildly non-polynomial behaviour for invertible 7×7 matrices with constrained support over $\mathbf{F}_q$.

Counting matrices by rank: wilderness



Theorem

(Belkale and Brosnan 2003)

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

Higman's conjecture

Definition

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

Conjecture

(Higman 1960)

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

Example

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

Theorem

(Vera-López and Arregi 2003,
Pak and 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, ...

Graphical groups

Definition

(Combine Baer 1938 and Tutte 1947)

Let Γ be a graph with vertices $v_1, \ldots, v_n$. The **graphical group** $\mathbf{G}_\Gamma(\mathbf{Z})$ associated with Γ over $\mathbf{Z}$ is generated by the vertices $v_1, \ldots, v_n$ subject to the following relations:

- $v_i v_j = v_j v_i = 1$ whenever $v_i \not\sim v_j$.
- Commutators are central.

Example

$\mathbf{G}_{\bullet - \bullet}(\mathbf{Z}) \approx \mathrm{U}_3(\mathbf{Z})$.

Graphical groups

Definition

(Combine Baer 1938 and Tutte 1947)

Let Γ be a graph with vertices $v_1, \ldots, v_n$. The **graphical group** $\mathbf{G}_\Gamma(\mathbf{Z})$ associated with Γ over $\mathbf{Z}$ is generated by the vertices $v_1, \ldots, v_n$ subject to the following relations:

- $v_i v_j = v_j v_i = 1$ whenever $v_i \not\sim v_j$. ⬅ RAAG/graph group
- Commutators are central.

Example

$\mathbf{G}_{\bullet\!-\!\bullet}(\mathbf{Z}) \approx \mathrm{U}_3(\mathbf{Z})$.

Graphical group schemes

Using commutator calculus à la P. Hall and Mal'cev, the definition above can be extended to define a group

$$\mathbf{G}_\Gamma(R)$$

for each (commutative) ring R.

This turns $\mathbf{G}_\Gamma$ into a (unipotent) group scheme which we call the **graphical group scheme** associated with Γ.

Graph Polynomiality Theorem

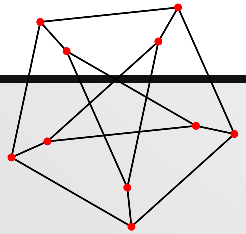
(R. & Voll 2019)

For every graph Γ, there exists a polynomial $f_\Gamma(X)$ such that for each prime power q,

$$\mathrm{k}(\mathbf{G}_\Gamma(\mathbf{F}_q)) = f_\Gamma(q).$$

Example

$$\begin{aligned} f_{\text{Petersen}}(X) = {} & X^{16} + X^{15} + 15X^{14} + 50X^{13} - 165X^{12} \\ & + 70X^{11} + 115X^{10} - 120X^{9} + 35X^{8} - X^{6} \end{aligned}$$



Polynomiality is unexpected (?!)

Definition

Given Γ with vertices $v_1, \ldots, v_n$, let $M_\Gamma(R)$ be the module of alternating $n \times n$ matrices $[a_{ij}]$ over R with $a_{ij} = 0$ whenever $v_i \not\sim v_j$.

Proposition

(R. & Voll 2019)

Let Γ have m edges. Then:

$$\mathrm{k}(\mathbf{G}_\Gamma(\mathbf{F}_q)) = q^m \cdot \text{average size of the kernel of } a \in M_\Gamma(\mathbf{F}_q)$$

$\int \text{wild} = \text{polynomial}$

- Let $\mathrm{Sym}_n(\mathbf{F}_q; S)$ be the space of symmetric $n \times n$ matrices $[a_{ij}]$ with $a_{ij} = 0$ whenever $(i,j) \notin S$.
- Let $\mathrm{Sym}_{n,r}(\mathbf{F}_q; S)$ be the subset of matrices of rank r.

Belkale & Brosnan 2004:

$\#\mathrm{Sym}_{n,r}(\mathbf{F}_q; S)$ is arbitrarily wild as a function of q.

R. & Voll 2019:

$\sum\limits_{r=0}^{n} \#\mathrm{Sym}_{n,r}(\mathbf{F}_q; S)\, q^{n-r}$ is a polynomial in q.

Class counting zeta functions

Definition

(du Sautoy 2004)

Let $\mathbf{G}$ be a group scheme (of finite type) over a ring R.

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

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

Example

(Berman et al. 2013, R. 2018)

$\zeta^{\mathrm{cc}}_{\mathrm{U}_3}(s) = \zeta(s-1)\zeta(s-2)/\zeta(s)$

Lemma (Euler product)

Let $\mathcal{O}$ be the ring of integers of a global field K.

Let $\mathbf{G}$ be a group scheme over $\mathcal{O}$. Then:

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

Theorem

(≈ du Sautoy 2004)

If $\mathcal{O} = \mathbf{Z}$, then $\zeta^{\mathrm{cc}}_{\mathbf{G} \otimes \mathbf{Z}_p}(s) \in \mathbf{Q}(p^{-s})$ for each prime p.

GIGO Theorem

If K is a number field, then $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathcal{O}_v}(\boldsymbol{s})$ "depends geometrically" on the place v whenever $\mathbf{G}$ is

- a Chevalley group (Berman et al. 2013) or
- unipotent (R. 2018).

GIGO Theorem

If K is a number field, then $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathcal{O}_v}(s)$ "depends geometrically" on the place v whenever $\mathbf{G}$ is

- a Chevalley group (Berman et al. 2013) or
- unipotent (R. 2018).

For such group schemes $\mathbf{G}$, 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 $v \in \mathcal{V}_K$,

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

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

Question

- How can one explicitly compute such formulae?

  The proof for unipotent groups is constructive but impractical.

  Practical methods: R. 2016–2020. Later!
- What about other group schemes?
- How wild can this geometry be?

Theorem

(Ishitsuka 2017 + R. 2020)

A positive proportion of elliptic curves over $\mathbf{Q}$ "appear" in class counting zeta functions of unipotent groups.

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 $\mathfrak{O}$ (e.g. $\mathbf{Z}_p$ or $\mathbf{F}_q[\![z]\!]$),

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

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

Remark

- $W_\Gamma(X,T) = 1 + f_\Gamma(X)T + \mathcal{O}(T^2)$.
- Our proof is constructive and gives rise to a practical algorithm.

Uniformity Theorem

(R. & Voll 2019)

F ... ists $W_\Gamma(X,T) \in \mathbf{Q}(X,T) \cap \mathbf{Q}[X][\![T]\!]$

... n ring $\mathfrak{O}$ (e.g. $\mathbf{Z}_p$

where q is the

Combinatorics in, combinatorics out!

Remark

- $W_\Gamma(X,T) = 1 + f_\Gamma(X)T + \mathcal{O}(T^2)$.
- Our proof is constructive and gives rise to a practical algorithm.

A new (?) graph invariant

Theorem

(R. & Voll 2019)

- Functional equation:
  $W_\Gamma(X^{-1}, T^{-1}) = -X^{n+m}T \cdot W_\Gamma(X, T)$,
  where $n =$ #vertices and $m =$ #edges
- Reduced zeta function:
  $W_\Gamma(1, T) = 1/(1 - T)$
- Hadamard products:
  $W_{\Gamma \oplus \Gamma'}(X, T) = W_\Gamma(X, T) \bigstar W_{\Gamma'}(X, T)$

Question

What does $W_\Gamma(X, T)$ tell us about Γ?

Cographs

Definition

Cographs are recursively defined as follows:

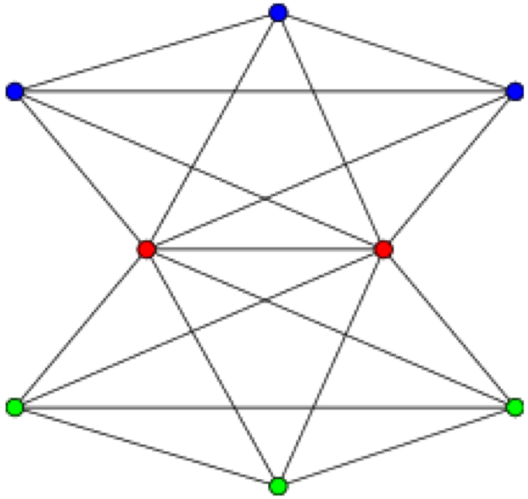
- A graph consisting of a single vertex is a cograph.
- If Γ and Γ' are cographs, then so are their disjoint union $\Gamma \oplus \Gamma'$ and join $\Gamma \vee \Gamma'$.

Theorem

(Corneil, Lerchs, Stewart Burlingham 1981)

A graph is a cograph iff it does not contain a path on four vertices as an induced subgraph.

Title page (reprise)



$= (K_3 \oplus \mathrm{K}_3) \vee \mathrm{K}_2$,

a cograph

$$W_{(\mathrm{K}_3 \oplus \mathrm{K}_3) \vee \mathrm{K}_2}(X, T) = \frac{X^{31}T^2 + X^{18}T - 2X^{16}T - 2X^{15}T + X^{13}T + 1}{(1 - X^{20}T)(1 - X^{19}T)^2}$$

Theorem

(R. & Voll 2019)

Let Γ be a cograph with n vertices and m edges.

- Explicit formula for $W_\Gamma(X,T)$ in terms of weak orders on n symbols.
- The abscissa of convergence of $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma}(s)$ is an integer.
- For each compact DVR $\mathfrak{O}$, the real part of each pole of $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma \otimes \mathfrak{O}}(s)$ is an integer.

Questions:

- What do these integers mean?
- What happens for general graphs?

Behind the scenes

Sketch of proof of the Uniformity Theorem

Uniformity Theorem

Given Γ, there exists $W_\Gamma(X,T)$ with $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma \otimes \mathfrak{O}}(s) = W_\Gamma(q, q^{-s})$ for ...

Ingredients

- Linearisation.
- Average sizes of modules.
- Knuth duality.
- Adjacency modules.
- Toric geometry.

Linearising class counting

Lemma (Burnside?)

Let G be a finite group. Then

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

If G admits a good Lie theory, then this lemma linearises.

For example, centralisers become kernels.

Zeta functions of modules

Definition

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

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

Theorem

(Lins 2019, R. 2020)

Let $\mathbf{G}$ be a unipotent group scheme. Let $A(X)$ be a "commutator matrix" of $\mathrm{Lie}(\mathbf{G})$. Then, generically,

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

Computing $\zeta_{M(X)}(s)$ (sketch)

- Choose a presentation $M(X) \approx \mathrm{Coker}(A(X))$.
- Goal: control the size of specialisations of $M(X)$ over quotients of $\mathfrak{O}$. Easy if $A(X)$ is in “Smith normal form”!
- Morally: use resolution of singularities to determine all SNFs of specialisations of $A(X)$. Usually impractical!
- If we are lucky, we can use methods from toric geometry instead. Implemented in my package **Zeta** for SageMath: http://www.maths.nuigalway.ie/~rossmann/Zeta/

Computing $\zeta_{M(X)}(s)$ (sketch)

- Choose a presentation $M(X) \approx \mathrm{Coker}(A(X))$.
- Goal: control the size of specialisations of $M(X)$ over quotients of $\mathfrak{O}$. Easy if $A(X)$ is in “Smith normal form”!
- Morally: use resolution of singularities to determine all SNFs of specialisations of $A(X)$. Usually impractical!
- If we are lucky, we can use methods from toric geometry instead. Implemented in my package Zeta for SageMath: http://www.maths.nuigalway.ie/~rossmann/Zeta/

For graphical groups, we can do much better!

Combinatorial Uniformity 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 $I_1, \dots, I_\ell$.

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.

Knuth duality

Definition

Let $A(X) = \left[\sum_k a_{ijk} X_k\right]$ be a matrix of linear forms.

The **Knuth duals** of $A(X)$ are obtained by "shuffling the indices" i, j, k.

Theorem

(R. 2020)

Let $B(Y)$ be a Knuth dual of $A(X)$. Then

$$\zeta_{\mathrm{Coker}\,A(X)}(s) \sim \zeta_{\mathrm{Coker}\,B(Y)}(s).$$

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
$$\mathbf{Z}_\sigma = \mathbf{Z}[X^\omega : \omega \in \sigma^* \cap \mathbf{Z}^n] \supset \mathbf{Z}[X].$$

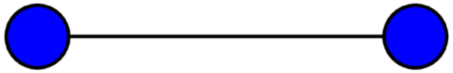
The Uniformity Theorem is a consequence of the following.

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 $\sigma \in \mathcal{F}$.

An illustration

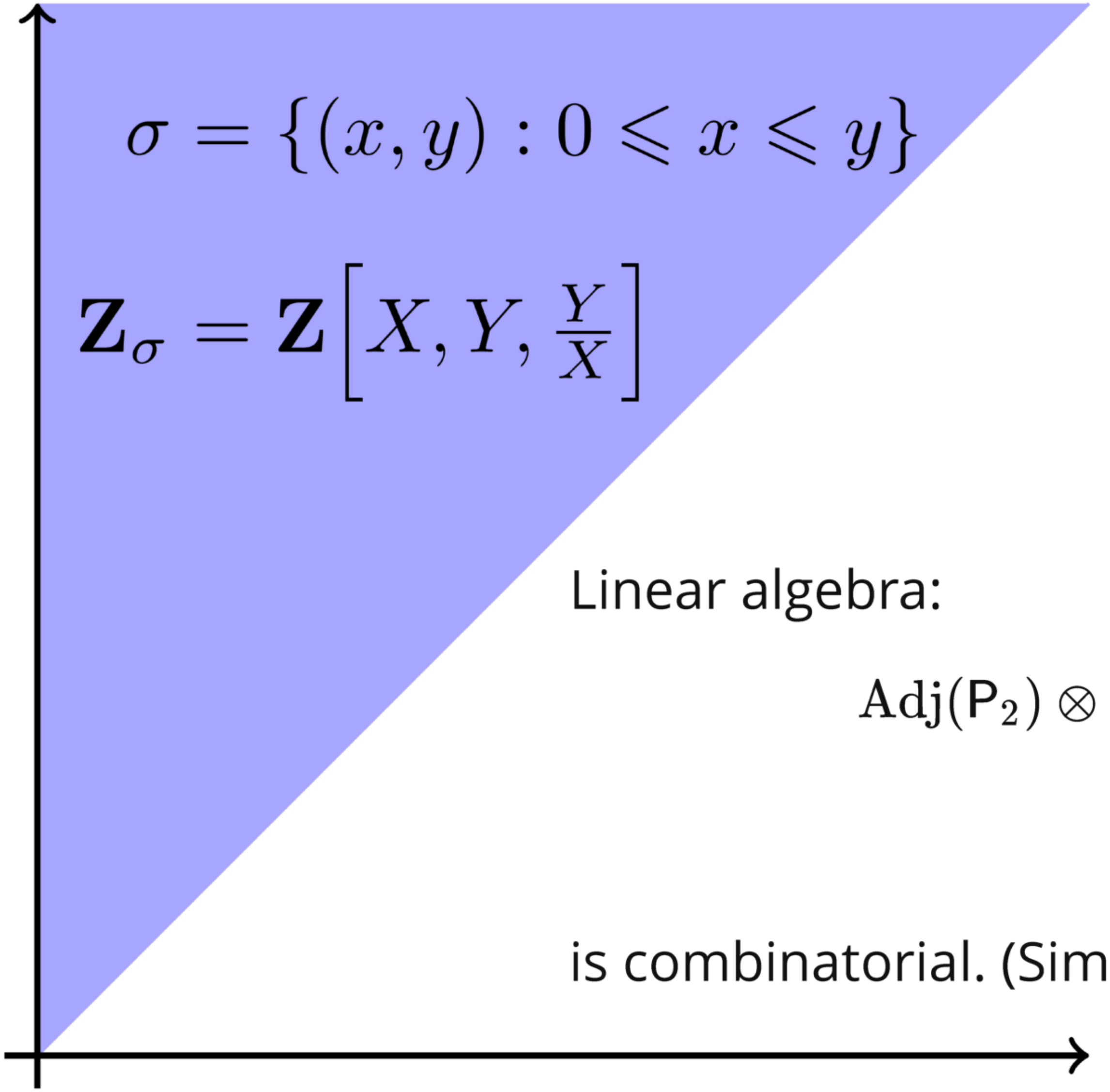
Let $\mathsf{P}_2 =$ 

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"!



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

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

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.)

Remarks

- Similar arguments works for all complete graphs.
- The case of general graphs is much more involved.

Our proof of the Uniformity Theorem is constructive.

An algorithmic version is available as part of Zeta.

Kite graphs

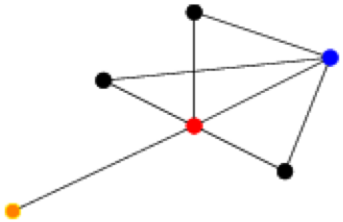
Definition

The class of kite graphs is recursively defined as follows:

- A graph $\bullet$ consisting of a single vertex is a kite graph.
- If Γ is a kite graph, then so are $\Gamma \oplus \bullet$ and $\Gamma \vee \bullet$.

Example

$\Gamma := (((\bullet \oplus \bullet \oplus \bullet) \vee \bullet) \oplus \bullet) \vee \bullet =$



is a kite graph with

$$\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma}(s) = \frac{\zeta(s-9)^2\zeta(s-10)}{\zeta(s-7)^2}.$$

Theorem

(R. & Voll 2019)

Let Γ be a kite graph.

- $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma}(s)$ is a product of finitely many factors $\zeta(s-a)^{\pm 1}$ for integers a (with explicit descriptions).
- $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma}(s)$ admits meromorphic continuation to all of $\mathbf{C}$.

Question

Do the conclusions of the preceding theorem characterise kite graphs?

Thank you

Advertisement

Groups in Galway meets the Irish Geometry Conference 2020

GiG 2020 meets IGC NUI Galway

May 14–16 2020, NUI Galway

Speakers include:

- Peter Brooksbank (Bucknell)
- Marston Conder (Auckland)
- James Cruickshank (Galway)
- Viveka Erlandsson (Bristol)
- Joanna Fawcett (London)
- Radhika Gupta (Bristol)
- Joshua Maglione (Bielefeld)
- Lucia Morotti (Hannover)
- John Murray (Maynooth)

Organisers: J. Burns, A. Carnevale, M. Kerin, T. Rossmann

More details: soon!