Distributions of modules over local finite $\mathbb{Z}_p$-algebras

Jack Klys

University of Calgary

May 11 2019

Random groups

- Let $\mathcal{S}$ be the set of finite abelian p-groups.
- One can define a probability meausure μ on $\mathcal{S}$ with $\sum_{A \in S} \mu(A) = 1$.
- In particular since

$$\eta^{-1} := \sum_{A \in \mathcal{S}} \frac{1}{|\mathrm{Aut} A|} = \prod_{i=1}^{\infty} \left(1 - p^{-i}\right)^{-1} < \infty$$

one can define the Cohen-Lenstra distribution on p-groups

$$\mu(A) = \frac{\eta}{|\mathrm{Aut} A|}.$$

Random groups

- An example:
- Let μ_n be Haar measure on $\mathbb{Z}_p$ extended to $M_n(\mathbb{Z}_p)$ the set of $n \times n$ matrices over $\mathbb{Z}_p$
- Then

$$\lim_{n \longrightarrow \infty} \mu_n \left(\{ M \in M_n(\mathbb{Z}_p) \mid \mathrm{coker} M \cong A \} \right) = \mu(A).$$

Random groups

- μ is characterized by the moments of the functions $f_A(X) = |\mathrm{Sur}(X, A)|$ for all $A \in \mathcal{S}$.

Proposition

If ν is any probability measure on $\mathcal{S}$ such that $\int_{\mathcal{S}} f_A d\nu = 1$ for all $A \in \mathcal{S}$ then $\nu = \mu$.

The function field setting

- Let C be a curve defined over a finite field $\mathbb{F}_q$ which is a finite cover of $\mathbb{P}^1_{\mathbb{F}_q}$
- Consider the Jacobian $\mathrm{Jac}\left(C\right)\left(\mathbb{F}_q\right) \cong \mathrm{Div}^0\left(C\right)/\mathrm{P}\left(C\right)$. This is a finite group.
- Let $\mathcal{M}_g$ be the set of hyperelliptic curves over $\mathbb{F}_q$ of genus g branched at ∞.

The function field setting

- We can consider, for $A \in \mathcal{S}$ and fixed g

$$\mu_g(A) = \frac{\left|\left\{C \in \mathcal{M}_g \mid \mathrm{Jac}(C)_p(\mathbb{F}_q) \cong A\right\}\right|}{|\mathcal{M}_g|}.$$

- Does $\lim_{g \longrightarrow \infty} \mu_g(A)$ exist?
- Function field analog of Cohen-Lenstra conjectures:

$$\lim_{g \longrightarrow \infty} \mu_g(A) = \mu(A)$$

Ellenberg-Venkatesh-Westerland

- As a consequence of proving bounds for dimensions of homology groups of Hurwitz spaces they were able to prove

Theorem 1 (Ellenberg-Venkatesh-Westerland (2016))

Fix $A \in \mathcal{S}$. Let $\delta_q^+ = \limsup_{g \longrightarrow \infty} \mu_g(A)$ and $\delta_q^- = \liminf_{g \longrightarrow \infty} \mu_g(A)$. Then $\lim_{q \longrightarrow \infty} \delta_q^{\pm} = \eta / |\mathrm{Aut} A| = \mu(A)$.

What about R-modules?

- Let R be a local ring containing $\mathbb{Z}_p$ which is finitely generated over $\mathbb{Z}_p$. Let $\mathbb{F}_R$ be its residue field.
- Let $\mathcal{S}_R$ be the set of finite p^∞-torsion R-modules
- Lipnowski and Tsimerman defined a measure μ_R on $\mathcal{S}_R$, extending the Cohen-Lenstra measure: For any integer N define $\mu_{R,N}$ to be the measure on $\mathcal{S}_R$ coming from cokernels of Haar-random matrices over R. Then $\mu_R = \lim_{N \longrightarrow \infty} \mu_{R,N}$.

What about R-modules?

- μ_R is supported on a subset of modules $T_R \subset \mathcal{S}_R$ and for $M \in T_R$, μ_R is defined by

$$\mu_R(M) = \frac{\eta_R}{|\mathrm{Aut}\, M|}$$

  where $\eta_R = \prod_{i=1}^{\infty}\left(1 - |\mathbb{F}_R|^{-i}\right)$.
- Similarly to μ, μ_R is also determined by the moments $\int_{\mathcal{S}_R} f_A d\nu = 1$ for all $A \in \mathcal{S}_R$.

Finite etale group schemes

- Let F be the Frobenius on a curve C
- We can ask about the distribution of $\mathrm{Jac}(C)/P(F)$ as an $R = \mathbb{Z}_p[F]/P(F)$ module for certain polynomials P.
- The category of $\mathbb{Z}_p\left[\mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)\right]$-modules is equivalent to the category of etale p-group schemes defined over $\mathbb{F}_q$.

An extension of EVW

- For G a finite etale p-group scheme over $\mathbb{F}_q$ let $\mathrm{Avg}(G, g, q)$ be the average number of surjections from $\mathrm{Jac}(C)$ to G (as group-schemes) over all $C \in \mathcal{M}_g$.

Theorem 2 (Lipnowski-Tsimerman(2019))

Let $\alpha_q^+ = \limsup_{g \longrightarrow \infty} \mathrm{Avg}(G, g, q)$ and $\alpha_q^- = \liminf_{g \longrightarrow \infty} \mathrm{Avg}(G, g, q)$. Then $\lim_{q \longrightarrow \infty} \alpha_q^{\pm} = 1$.

Comparison of the results

- Notice EVW's theorem is a statement about $\mu_g(A)$ whereas Lipnowski-Tsimerman is a statement about $\mathrm{Avg}(G, g, q)$.
- Analogous to the group setting, for $R = \mathbb{Z}_p[X]/P(X)$ and $A \in \mathcal{S}_R$ define

$$\mu_{g,R}(A) = \frac{\left|\left\{C \in \mathcal{M}_g \mid \mathrm{Jac}(C)_p / P(F) \cong A\right\}\right|}{|\mathcal{M}_g|}.$$

- By definition $\mathrm{Avg}(G, g, q) = \int_{\mathcal{S}_R} f_A \mu_{g,R}$.

From moments to measures

- To go from $\mathrm{Avg}(G, g, q)$ to $\mu_{g,R}(A)$ need a result of the form: convergence of moments $\Longrightarrow$ convergence of measures.
- In the setting of groups:

Theorem 3 (Ellenberg-Venkatesh-Westerland (2016))

If $\{\nu_n\}$ is a sequence of probability measures on $\mathcal{S}$ such that $\int_{\mathcal{S}} f_A d\nu_n \longrightarrow 1$ for all $A \in \mathcal{S}$ then $\nu_n(A) \longrightarrow \mu(A)$ for all $A \in \mathcal{S}$.

From moments to measures

- Key fact needed to prove Theorem 3:

Proposition (Ellenberg-Venkatesh-Westerland (2016))

For any $\epsilon > 0$ and $A \in \mathcal{S}$ there exists a finite set $T \subset \mathcal{S}$ and $c \in \mathbb{N}$ such that for all X with $|X| > c$

$$f_A(X) \leq \epsilon \cdot \frac{\sum_{A' \in T} f_{A'}(X)}{|T|}.$$

- Integrating the above gives $\int_{|X|>c} f_A(X)\, d\mu_g \leq \epsilon$ for all large enough g, that is there is no 'escape of mass'.

Proof sketch

Proof sketch

- Define A' to be an *s-enlargement* of A if there is a surjection $A' \longrightarrow A$ with kernel of size p^s. Let $E_s(A)$ be the set of s-enlargements of A.
- Show that if X is large enough then there exists $A' \in E_s(A)$

$$f_{A'}(X) \geq (p-1)^s f_A(X)$$

.

Proof sketch

Proof sketch continued

- Then for any X large enough

$$\left|E_s(A)\right| \frac{\sum_{A' \in E_s(A)} f_{A'}(X)}{\left|E_s(A)\right|} \geq f_{A'}(X) \geq (p-1)^s f_A(X)$$

- It is easy to see $\left|E_s(A)\right| \leq \mathcal{P}(s + \mathrm{rk} A)$ where $\mathcal{P}(n)$ is the number of partitions of n and that $\mathcal{P}(s + \mathrm{rk} A) / (p-1)^s \longrightarrow 0$ as $s \longrightarrow \infty$. So let $\epsilon = \left|E_s(A)\right| / (p-1)^s$.

The property of 'few enlargements'

- This proof mostly works for R-modules, except: it is not necessarily true that $|E_s(A)|$ is sub-exponential in s for $A \in \mathcal{S}_R$.
- Say a ring R has the property of *few enlargements* if $E_s(M)$ grows sub-exponentially in s for every R-module M

Obtaining a bound

- Obtaining a bound (assume $R = \mathbb{Z}_p[X]/P(X)$ for some polynomial P):
- Suppose $I \subset \mathbb{Z}_p[X]$ is an ideal such that $S = \mathbb{Z}_p[X]/I$ has few-enlargements. Then so does $R_k = R/I^k$ for any k.
- Since R_k has few-enlargements we have $\lim_{g \longrightarrow \infty} \mu_{g,R_k} = \mu_{R_k}$ by Lipnowski-Tsimerman
- Furthermore $\lim_{k \longrightarrow \infty} \mu_{R_k} = \mu_R$.

Obtaining a bound

- It follows from the definition of $\mu_{g,R}$ that if $R \twoheadrightarrow R_k$ and M is an R_k-module then $\mu_{g,R}(M) < \mu_{g,R_k}(M)$.
- Hence

$$\mu_{R_k} = \lim_{g \longrightarrow \infty} \mu_{g,R_k} > \lim_{g \longrightarrow \infty} \mu_{g,R}$$

  and taking limit in k gives

$$\mu_R > \lim_{g \longrightarrow \infty} \mu_{g,R}.$$

A different approach

- Modify EVW's proof to not use all enlargements
- Let $N_s(A) \subset E_s(A)$ be the minimal subset satisfying: for all $M \in \mathcal{S}_R$ large enough, if $f_A(M) > 0$ then $f_{A'}(M) > 0$ for some $A' \in N_s(A)$.
- Let $n_s(A) = |N_s(A)|$.

Theorem 1 for R-modules

Theorem (K.)

If $n_s(A)/(|\mathbb{F}_R|-1)^s \longrightarrow 0$ as $s \longrightarrow \infty$ then Theorem 1 is true for $\mathcal{S}_R$.

If R is a PID then $n_s(A) = \mathrm{rk} A + 2$.

In general

$$n_s(A) \leq (\mathrm{rk} A + s(s+1)/2) \times \max_{M \in N_s(A)} |\mathrm{Hom}(R, \mathrm{End}_{\mathbb{Z}}(M))/\sim \mathrm{Aut}_{\mathbb{Z}}(M)|$$

for $A \in \mathcal{S}_R$.

Theorem 1 for R-modules

proof sketch

- As before we want to show for any $A \in \mathcal{S}_R$ and $\epsilon > 0$ that

$$\int_{|X|>c} f_A(X)\, d\mu_g \leq \epsilon$$

  for all large enough g.
- Partition the set of X into disjoint subsets $T_{A'}$ indexed by $A' \in N_s(A)$. $T_{A'}$ consists of elements X satisfying $f_{A'}(X) = g(X)\, f_A(X)$ and $g(X) \geq (|\mathbb{F}_R| - 1)^s$

Theorem 1 for R-modules

proof sketch continued

- For some $\delta > 0$

$$\int_{|X|>c} f_A(X)\, d\mu_g = \sum_{A' \in N_s(A)} \int_{X \in T_{A'}} \frac{1}{g(X)} f_{A'}(X)\, d\mu_g$$
$$< \frac{n_s(A)}{(|\mathbb{F}_R| - 1)^s}(1+\delta)$$
$$< \epsilon$$

since $n_s(A)/g(X) \leq n_s(A)/(|\mathbb{F}_R| - 1)^s \longrightarrow 0$ as $s \longrightarrow \infty$.

Question: What is the growth of
$|\mathrm{Hom}(R, \mathrm{End}_{\mathbb{Z}}(M))/\sim \mathrm{Aut}_{\mathbb{Z}}(M)|$ as $s \longrightarrow \infty$.

Thank you!