# Probability theory for random groups arising in number theory

Melanie Matchett Wood
includes joint work with Weitong Wang, Will Sawin, Hoi Nguyen

Harvard University

International Congress of Mathematicians 2022

# Overview

1. Motivating examples of random groups
2. The moment problem for random groups
3. Universality for random groups

# Overview

# Distributions of groups arising in number theory and related contexts

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields,

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$,

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family),

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family), what is the distribution of $\mathrm{Sel}_p(E)$?

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family), what is the distribution of $\mathrm{Sel}_p(E)$?
   (controls the rational solutions $(x, y) \in \mathbb{Q}^2$ of $y^2 = x^3 + ax + b$)

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family), what is the distribution of $\mathrm{Sel}_p(E)$?
   (controls the rational solutions $(x, y) \in \mathbb{Q}^2$ of $y^2 = x^3 + ax + b$)
3. If $M$ is a random $n \times n$ matrix with each entry independent uniform from $\{0, 1\}$,

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family), what is the distribution of $\mathrm{Sel}_p(E)$?
   (controls the rational solutions $(x, y) \in \mathbb{Q}^2$ of $y^2 = x^3 + ax + b$)
3. If $M$ is a random $n \times n$ matrix with each entry independent uniform from $\{0, 1\}$, so $M : \mathbb{Z}^n \to \mathbb{Z}^n$,

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family), what is the distribution of $\mathrm{Sel}_p(E)$?
   (controls the rational solutions $(x, y) \in \mathbb{Q}^2$ of $y^2 = x^3 + ax + b$)
3. If $M$ is a random $n \times n$ matrix with each entry independent uniform from $\{0, 1\}$, so $M : \mathbb{Z}^n \to \mathbb{Z}^n$, what is the distribution of $\mathbb{Z}^n / M(\mathbb{Z}^n)$?

# Distributions of groups arising in number theory and related contexts

1. As $K$ varies over some collection of number fields, what is the distribution of $\mathrm{Cl}_K$?
   (a group that controls factorization in algebraic integers of $K$)
   E.g., take a uniform random square-free integer $D \in [2, X]$, let $K = \mathbb{Q}(\sqrt{D})$ (especially interesting as $X \to \infty$)
   For a prime $p$, we might ask about the $p$-torsion $\mathrm{Cl}_K[p]$ or the Sylow $p$-subgroup
2. As $E$ varies over some collection of elliptic curves $/\mathbb{Q}$ (e.g. all of them, or a quadratic twist family), what is the distribution of $\mathrm{Sel}_p(E)$?
   (controls the rational solutions $(x, y) \in \mathbb{Q}^2$ of $y^2 = x^3 + ax + b$)
3. If $M$ is a random $n \times n$ matrix with each entry independent uniform from $\{0, 1\}$, so $M : \mathbb{Z}^n \to \mathbb{Z}^n$, what is the distribution of $\mathbb{Z}^n / M(\mathbb{Z}^n)$?
   Related: what is the distribution of the Jacobian of an Erdős–Rényi random graph (i.e. sandpile group, i.e. $\mathbb{Z}^n / \Delta(\mathbb{Z}^n)$ where $\Delta$ is the graph Laplacian)

# Distributions of groups arising in number theory and related contexts

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$,

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
(Function field analog of the class group question)

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
   (Function field analog of the class group question)
   Or the distribution of $\pi_1^{alg}(C)$?

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
   (Function field analog of the class group question)
   Or the distribution of $\pi_1^{alg}(C)$?
5. As $K$ varies over some number fields,

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
   (Function field analog of the class group question)
   Or the distribution of $\pi_1^{alg}(C)$?
5. As $K$ varies over some number fields, if $K^{un}$ is the maximal unramified extension of $K$,

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
   (Function field analog of the class group question)
   Or the distribution of $\pi_1^{alg}(C)$?
5. As $K$ varies over some number fields, if $K^{un}$ is the maximal unramified extension of $K$, what is the distribution of $\mathrm{Gal}(K^{un}/K) = \pi_1^{alg}(\mathrm{Spec}\,\mathcal{O}_K)$?

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
   (Function field analog of the class group question)
   Or the distribution of $\pi_1^{alg}(C)$?
5. As $K$ varies over some number fields, if $K^{un}$ is the maximal unramified extension of $K$, what is the distribution of $\mathrm{Gal}(K^{un}/K) = \pi_1^{alg}(\mathrm{Spec}\,\mathcal{O}_K)$?
6. As $M$ varies over 3-manifolds (e.g. in the Dunfield-Thurston model of random Heegaard splittings),

# Distributions of groups arising in number theory and related contexts

4. As $C$ varies over some collection of curves over finite field $\mathbb{F}_q$, what is the distribution of $\mathrm{Pic}(C)$?
   (Function field analog of the class group question)
   Or the distribution of $\pi_1^{alg}(C)$?
5. As $K$ varies over some number fields, if $K^{un}$ is the maximal unramified extension of $K$, what is the distribution of $\mathrm{Gal}(K^{un}/K) = \pi_1^{alg}(\mathrm{Spec}\,\mathcal{O}_K)$?
6. As $M$ varies over 3-manifolds (e.g. in the Dunfield-Thurston model of random Heegaard splittings), what is the distribution of $\pi_1(M)$?

# Overview

# Recognizing distributions of real numbers from moments

# Recognizing distributions of real numbers from moments

When we have a distribution of numbers, we often can recognize the distribution by its *moments*.

# Recognizing distributions of real numbers from moments

When we have a distribution of numbers, we often can recognize the distribution by its *moments*.

$k$th moment: $M_k :=$ average of $x^k$,

# Recognizing distributions of real numbers from moments

When we have a distribution of numbers, we often can recognize the distribution by its *moments*.

$k$th moment: $M_k :=$ average of $x^k$, i.e. $\int_x x^k d\mu$,

# Recognizing distributions of real numbers from moments

When we have a distribution of numbers, we often can recognize the distribution by its *moments*.

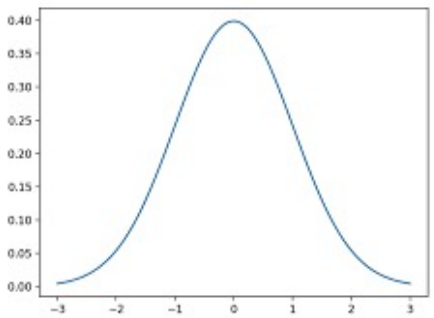
$k$th moment: $M_k :=$ average of $x^k$, i.e. $\int_x x^k d\mu$, i.e. $\mathbb{E}[X^k]$

# Recognizing distributions of real numbers from moments

When we have a distribution of numbers, we often can recognize the distribution by its *moments*.

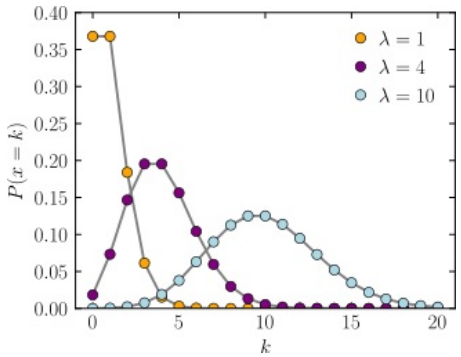
$k$th moment: $M_k :=$ average of $x^k$, i.e. $\int_x x^k d\mu$, i.e. $\mathbb{E}[X^k]$

Gaussian distribution:



$$\mathbb{E}[(X-\mu)^k] = \begin{cases} 0 & k \text{ odd} \\ \sigma^k(k-1)!! & k \text{ even} \end{cases}$$

Poisson distribution:



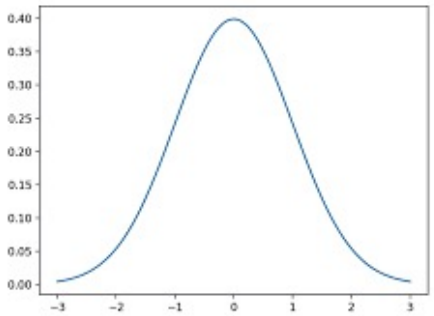

$$\mathbb{E}[X(X-1)\cdots(X-k)] = \lambda^k$$

# Recognizing distributions of real numbers from moments

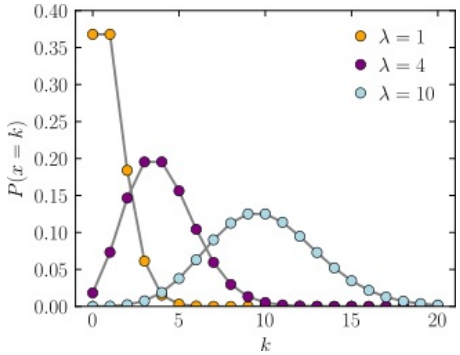
When we have a distribution of numbers, we often can recognize the distribution by its *moments*.

$k$th moment: $M_k :=$ average of $x^k$, i.e. $\int_x x^k d\mu$, i.e. $\mathbb{E}[X^k]$

Gaussian distribution:



Poisson distribution:




$$\mathbb{E}[(X-\mu)^k] = \begin{cases} 0 & k \text{ odd} \\ \sigma^k (k-1)!! & k \text{ even} \end{cases}$$

$$\mathbb{E}[X(X-1)\cdots(X-k)] = \lambda^k$$

Knowledge of $\mathbb{E}[X]$ and these up to $k$ is equivalent to knowledge of first $k$ moments

# Recognizing distributions of real numbers from moments

# Recognizing distributions of real numbers from moments

**Theorem (Uniqueness of the moment problem)**

*When the moments don't grow too fast,*

# Recognizing distributions of real numbers from moments

**Theorem (Uniqueness of the moment problem)**

*When the moments don't grow too fast, then there is at most* 1 *distribution with those moments.*

# Recognizing distributions of real numbers from moments

**Theorem (Uniqueness of the moment problem)**

*When the moments don't grow too fast, then there is at most* 1 *distribution with those moments.*

$M_k = e^k$ is not too fast, but $M_k = e^{k^2}$ is too fast

# Recognizing distributions of real numbers from moments

**Theorem (Uniqueness of the moment problem)**

*When the moments don't grow too fast, then there is at most* 1 *distribution with those moments.*

$M_k = e^k$ is not too fast, but $M_k = e^{k^2}$ is too fast

Moments are often much more accessible than direct information about the distribution

# Moments of random groups

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

Just treat $V$ as $|V|$

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

Just treat $V$ as $|V|$

Then $M_k \approx 2^{k^2/4}$, too large to apply moment problem for numbers

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

Just treat $V$ as $|V|$

Then $M_k \approx 2^{k^2/4}$, too large to apply moment problem for numbers

1. There was a candidate distribution, with distribution and moments known explicitly

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

Just treat $V$ as $|V|$

Then $M_k \approx 2^{k^2/4}$, too large to apply moment problem for numbers

1. There was a candidate distribution, with distribution and moments known explicitly
2. Authors proved moments matched candidate distribution

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

Just treat $V$ as $|V|$

Then $M_k \approx 2^{k^2/4}$, too large to apply moment problem for numbers

1. There was a candidate distribution, with distribution and moments known explicitly
2. Authors proved moments matched candidate distribution
3. Proved new theorem that moments determine distribution

# Moments of random groups

Heath-Brown '94 on 2-Selmer groups of $y^2 = x^3 - Dx$ ($D$ square-free $\in \mathbb{Z}$)

Fouvry-Klüners '06 on $2\,\mathrm{Cl}_K\,/4\,\mathrm{Cl}_K$ as $K$ varies over $\mathbb{Q}(\sqrt{D})$

Both are distributions on $\mathbb{F}_2$-vector spaces, i.e. random $\mathbb{F}_2$-vector spaces

Just treat $V$ as $|V|$

Then $M_k \approx 2^{k^2/4}$, too large to apply moment problem for numbers

1. There was a candidate distribution, with distribution and moments known explicitly
2. Authors proved moments matched candidate distribution
3. Proved new theorem that moments determine distribution

# Moments of random (pro)-finite groups, modern theory

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

*then $X$ and $Y$ have the same distribution.*

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

*then $X$ and $Y$ have the same distribution.*

Application:

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

*then $X$ and $Y$ have the same distribution.*

Application: (Ellenberg, Venkatesh, Westerland '16; Liu, W., Zureick-Brown '19)

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

*then $X$ and $Y$ have the same distribution.*

Application: (Ellenberg, Venkatesh, Westerland '16; Liu, W., Zureick-Brown '19) to $\operatorname{Pic}(C)$ of curves $C$ over finite fields $\mathbb{F}_q$,

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

*then $X$ and $Y$ have the same distribution.*

Application: (Ellenberg, Venkatesh, Westerland '16; Liu, W., Zureick-Brown '19) to $\operatorname{Pic}(C)$ of curves $C$ over finite fields $\mathbb{F}_q$, function field Cohen-Lenstra-Martinet for $q \to \infty$

# Moments of random (pro)-finite groups, modern theory

- indexed by *finite groups*, instead of by natural numbers
- moments themselves are numbers
- $G$th moment: $M_G(X) := \mathbb{E}[\#\operatorname{Sur}(X, G)]$ or $M_G(\mu) := \int_X \#\operatorname{Sur}(X, G) d\mu$

**Theorem (Uniqueness of the moment problem for finite abelian groups, Wang-W. '21)**

*Let $X, Y$ be random finite abelian groups. If for each finite ab. group $A$,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) = O(|\wedge^2 A|),$$

*then $X$ and $Y$ have the same distribution.*

Application: (Ellenberg, Venkatesh, Westerland '16; Liu, W., Zureick-Brown '19) to $\operatorname{Pic}(C)$ of curves $C$ over finite fields $\mathbb{F}_q$, function field Cohen-Lenstra-Martinet for $q \to \infty$
(EVW applied their own version for $p$-Sylow subgroups, LWZB applied analog for finite abelian $R$-modules)

# Moment problem for groups, modern theory

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

New approach (Sawin-W.) to construct a distribution of random groups explicitly from moments

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

New approach (Sawin-W.) to construct a distribution of random groups explicitly from moments

Application (Sawin-W.): find the distribution of (profinite completions of) fundamental groups of random 3-manifolds, with explicit formulas

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

New approach (Sawin-W.) to construct a distribution of random groups explicitly from moments

Application (Sawin-W.): find the distribution of (profinite completions of) fundamental groups of random 3-manifolds, with explicit formulas

*S-group*: a group whose order is a product of powers of primes in $S$

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

New approach (Sawin-W.) to construct a distribution of random groups explicitly from moments

Application (Sawin-W.): find the distribution of (profinite completions of) fundamental groups of random 3-manifolds, with explicit formulas

*S-group*: a group whose order is a product of powers of primes in $S$

## Corollary (Sawin-W., '22)

*Let $S$ be a finite set of primes.*

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

New approach (Sawin-W.) to construct a distribution of random groups explicitly from moments

Application (Sawin-W.): find the distribution of (profinite completions of) fundamental groups of random 3-manifolds, with explicit formulas

*S-group*: a group whose order is a product of powers of primes in $S$

## Corollary (Sawin-W., '22)

*Let $S$ be a finite set of primes. For a random (compact, without boundary) 3-manifold $M$ from Dunfield-Thurston's model of random Heegaard splittings,*

# Moment problem for groups, modern theory

What if you don't know an explicit distribution with the moments you find?

New approach (Sawin-W.) to construct a distribution of random groups explicitly from moments

Application (Sawin-W.): find the distribution of (profinite completions of) fundamental groups of random 3-manifolds, with explicit formulas

*S-group*: a group whose order is a product of powers of primes in $S$

## Corollary (Sawin-W., '22)

*Let $S$ be a finite set of primes. For a random (compact, without boundary) 3-manifold $M$ from Dunfield-Thurston's model of random Heegaard splittings,*

$$\text{Prob}(\pi_1(M) \text{ has no non-trivial } S\text{-group quotients})$$
$$= \prod_{p \in S} \prod_{j \geq 1} (1 + p^{-j})^{-1} \prod_{\substack{N \text{ non-ab. finite} \\ \text{simple } S\text{-group}}} e^{-\frac{|H_2(N,\mathbb{Z})|}{|\text{Out}(N)|}}.$$

# Overview

# Universality: the Central Limit Theorem

# Universality: the Central Limit Theorem

## Theorem (Central Limit Theorem)

*Let $X_1, X_2, \ldots$ be independent, identically distributed random real numbers with finite mean $\mu = \mathbb{E}(X_i)$ and finite variance $\sigma^2$.*

# Universality: the Central Limit Theorem

## Theorem (Central Limit Theorem)

*Let $X_1, X_2, \ldots$ be independent, identically distributed random real numbers with finite mean $\mu = \mathbb{E}(X_i)$ and finite variance $\sigma^2$. Then as $n \to \infty$,*

# Universality: the Central Limit Theorem

## Theorem (Central Limit Theorem)

*Let $X_1, X_2, \ldots$ be independent, identically distributed random real numbers with finite mean $\mu = \mathbb{E}(X_i)$ and finite variance $\sigma^2$. Then as $n \to \infty$,*

$$\sqrt{n}\left(\frac{X_1 + \cdots + X_n}{n} - \mu\right)$$

# Universality: the Central Limit Theorem

## Theorem (Central Limit Theorem)

*Let $X_1, X_2, \ldots$ be independent, identically distributed random real numbers with finite mean $\mu = \mathbb{E}(X_i)$ and finite variance $\sigma^2$. Then as $n \to \infty$,*

$$\sqrt{n}\left(\frac{X_1 + \cdots + X_n}{n} - \mu\right)$$

*converge in distribution to the normal distribution with mean 0 and variance $\sigma^2$.*

# Universality: the Central Limit Theorem

**Theorem (Central Limit Theorem)**

*Let $X_1, X_2, \ldots$ be independent, identically distributed random real numbers with finite mean $\mu = \mathbb{E}(X_i)$ and finite variance $\sigma^2$. Then as $n \to \infty$,*

$$\sqrt{n}\left(\frac{X_1 + \cdots + X_n}{n} - \mu\right)$$

*converge in distribution to the normal distribution with mean 0 and variance $\sigma^2$.*

The output distribution of this process that combines the $X_i$ is largely *insensitive* to the input distribution.

# Universality: random finite abelian groups

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers* $n, u \geq 0$ *and* $\epsilon > 0$,

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution,*

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ $from\ any\ distribution$, such that for every prime $p$,*

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution, such that for every prime $p$,*

$$\max_{a\in\mathbb{F}_p} \text{Prob}(x \equiv a \pmod{p}) \leq 1 - \epsilon.$$

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution, such that for every prime $p$,*

$$\max_{a\in\mathbb{F}_p} \text{Prob}(x \equiv a \pmod{p}) \leq 1 - \epsilon.$$

*For any fixed finite abelian group $A$ and $u \geq 0$,*

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution, such that for every prime $p$,*

$$\max_{a\in\mathbb{F}_p} \text{Prob}(x \equiv a \pmod{p}) \leq 1 - \epsilon.$$

*For any fixed finite abelian group $A$ and $u \geq 0$,*

$$\lim_{n\to\infty} \text{Prob}\left(\mathbb{Z}^n/(M_{n\times(n+u)}\mathbb{Z}^{n+u}) \simeq A\right) = \frac{1}{|A|^u |\,\text{Aut}(A)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1},$$

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution, such that for every prime $p$,*

$$\max_{a\in\mathbb{F}_p} \text{Prob}(x \equiv a \pmod{p}) \leq 1 - \epsilon.$$

*For any fixed finite abelian group $A$ and $u \geq 0$,*

$$\lim_{n\to\infty} \text{Prob}\left(\mathbb{Z}^n/(M_{n\times(n+u)}\mathbb{Z}^{n+u}) \simeq A\right) = \frac{1}{|A|^u |\,\text{Aut}(A)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1},$$

*where $\zeta(s)$ is the Riemann zeta function.*

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution, such that for every prime $p$,*

$$\max_{a\in\mathbb{F}_p} \text{Prob}(x \equiv a \pmod{p}) \leq 1 - \epsilon.$$

*For any fixed finite abelian group $A$ and $u \geq 0$,*

$$\lim_{n\to\infty} \text{Prob}\left(\mathbb{Z}^n/(M_{n\times(n+u)}\mathbb{Z}^{n+u}) \simeq A\right) = \frac{1}{|A|^u |\,\text{Aut}(A)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1},$$

*where $\zeta(s)$ is the Riemann zeta function.*

$\mathbb{Z}^n/(M_{n\times(n+u)}\mathbb{Z}^{n+u})$ is the quotient of a fixed free abelian group $\mathbb{Z}^n$,

# Universality: random finite abelian groups

## Theorem (Nguyen-W. '21)

*For integers $n, u \geq 0$ and $\epsilon > 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer $x$ from any distribution, such that for every prime $p$,*

$$\max_{a\in\mathbb{F}_p} \text{Prob}(x \equiv a \pmod{p}) \leq 1 - \epsilon.$$

*For any fixed finite abelian group $A$ and $u \geq 0$,*

$$\lim_{n\to\infty} \text{Prob}\left(\mathbb{Z}^n/(M_{n\times(n+u)}\mathbb{Z}^{n+u}) \simeq A\right) = \frac{1}{|A|^u |\,\text{Aut}(A)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1},$$

*where $\zeta(s)$ is the Riemann zeta function.*

$\mathbb{Z}^n/(M_{n\times(n+u)}\mathbb{Z}^{n+u})$ is the quotient of a fixed free abelian group $\mathbb{Z}^n$, by random relations (given by the columns of $M$)

# Universality: random finite abelian groups

# Universality: random finite abelian groups

Zoom out: quotient of fixed free abelian group $\mathbb{Z}^n$ by random relations,

# Universality: random finite abelian groups

Zoom out: quotient of fixed free abelian group $\mathbb{Z}^n$ by random relations, as $n \to \infty$ resulting distribution is largely insensitive to the distribution of the relations

# Universality: random finite abelian groups

Zoom out: quotient of fixed free abelian group $\mathbb{Z}^n$ by random relations, as $n \to \infty$ resulting distribution is largely insensitive to the distribution of the relations

Applications (of analogs for symmetric matrices):

# Universality: random finite abelian groups

Zoom out: quotient of fixed free abelian group $\mathbb{Z}^n$ by random relations, as $n \to \infty$ resulting distribution is largely insensitive to the distribution of the relations

Applications (of analogs for symmetric matrices):
Jacobians/sandpile groups of random graphs W. '17 (Erdős–Rényi), Mészáros '20 (uniform $d$-regular graphs $\implies$ non-singularity of adjacency matrix /$\mathbb{R}$)

# Universality: further random algebraic structures

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

1. Random finite abelian groups with additional structure (e.g. alternating pairing)

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

1. Random finite abelian groups with additional structure (e.g. alternating pairing)
2. Random finite or profinite groups

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

1. Random finite abelian groups with additional structure (e.g. alternating pairing)
2. Random finite or profinite groups
3. Random rings, modules, etc.

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

1. Random finite abelian groups with additional structure (e.g. alternating pairing)
2. Random finite or profinite groups
3. Random rings, modules, etc.
4. Allowing some dependence in the inputs

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

1. Random finite abelian groups with additional structure (e.g. alternating pairing)
2. Random finite or profinite groups
3. Random rings, modules, etc.
4. Allowing some dependence in the inputs
5. Allowing some degeneracy in the inputs

# Universality: further random algebraic structures

Sawin-W. 3-manifolds result allows some (minor) flexibility in how you build the random 3-manifold (in choice of generators for mapping class group)

Many open problems: can one prove universality for

1. Random finite abelian groups with additional structure (e.g. alternating pairing)
2. Random finite or profinite groups
3. Random rings, modules, etc.
4. Allowing some dependence in the inputs
5. Allowing some degeneracy in the inputs