Distributions of unramified extensions of global fields

David Zureick-Brown (Emory University)
Yuan Liu (University of Illinois Urbana-Champaign)
Melanie Matchett Wood (Harvard University)

Slides available at http://www.math.emory.edu/~dzb/slides/

Joint Mathematics Meetings
Special session on Arithmetic Statistics
January 5, 2023

Main problem: variation of K^{ur}

Fix a finite group Γ (e.g., $\Gamma = \mathbb{Z}/2\mathbb{Z}$).

$$
\begin{array}{l}
\mathrm{Gal}(K^{\mathrm{ur}}/K)\left\{\begin{array}{l}
K^{\mathrm{ur}} \\
\quad | \\
H \\
\quad | \ \mathrm{Gal}(H/K) \cong \mathrm{Gal}(K^{\mathrm{ur}}/K)^{\mathrm{ab}} \cong \mathrm{Cl}(K) \\
K
\end{array}\right. \\
\qquad\qquad\qquad\quad | \ \Gamma \cong \mathrm{Gal}(K/\mathbb{Q}) \\
\qquad\qquad\qquad\quad \mathbb{Q}
\end{array}
$$

Problem

1. *How do K^{ur} and $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ vary as K varies over Γ extensions?*
2. *How should we model K^{ur} and $\mathrm{Gal}(K^{\mathrm{ur}}/K)$?*

Class field towers

Setup

1. Let $K_0 = K$.
2. Let $K_i =$ the Hilbert class field of K_{i-1}.
3. Let $K_H = \bigcup_i K_i \subset K^{\mathrm{ur}}$.
4. Note that if $K_2 \neq K_1$ then $\mathrm{Gal}(K_2/K)$ is nonabelian.

$$\mathbb{Q} \subset K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_H \subset K^{\mathrm{ur}}$$

Examples (Hermite–Minkowski; Schoof, 1986; Lang)

$$\begin{array}{lcrcl} K = \mathbb{Q} & \Rightarrow & \mathbb{Q} & = & \mathbb{Q}^{ur} \\ K = \mathbb{Q}(\zeta_{877}) & \Rightarrow & [K^{\mathrm{ur}} : K] & = & \infty \\ K = \mathbb{Q}(\sqrt{2869}) & \Rightarrow & K_H & \neq & K^{\mathrm{ur}} \end{array}$$

Class field towers

Theorem (Golod–Shaferevich, 1964)

Let $K = \mathbb{Q}(\sqrt{-|D|})$. *Suppose that* $\mathrm{rk}(\mathrm{Cl}\,K)_2 \geq 5$. *Then* $[(K_H)_2 : K] = \infty$.

Theorem (Furuta, 1972)

Fix ℓ. *Let* $K = \mathbb{Q}(\zeta_n)$ *and suppose that* n *is divisible by at least* 8 *primes* p *such that* $\ell \mid p - 1$. *Then* $[(K_H)_\ell : K] = \infty$.

Main problem: variation of K^{ur}

Fix a finite group Γ (e.g., $\Gamma = \mathbb{Z}/2\mathbb{Z}$).

$$\mathrm{Gal}(K^{\mathrm{ur}}/K)\left\{\begin{array}{l} K^{\mathrm{ur}} \\ \Big| \\ H \\ \Big|\ \mathrm{Gal}(H/K)\cong\mathrm{Gal}(K^{\mathrm{ur}}/K)^{\mathrm{ab}}\cong\mathrm{Cl}(K) \\ K \end{array}\right.$$

$$\begin{array}{l} \Big|\ \Gamma\cong\mathrm{Gal}(K/\mathbb{Q}) \\ \mathbb{Q}\end{array}$$

Problem

1. *How do K^{ur} and $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ vary as K varies over Γ extensions?*
2. *How should we model K^{ur} and $\mathrm{Gal}(K^{\mathrm{ur}}/K)$?*

Variation (v.1)

Let $E_\Gamma(D)$ be the set of Γ-extensions K of $\mathbb{Q}$ with $\operatorname{rDisc} K = D$.

Let H be a profinite group.

Moments

$$\lim_{B\to\infty} \frac{\sum_{D\leq B} \sum_{K\in E_\Gamma(D)} |\mathrm{Sur}_\Gamma(\mathrm{Gal}(K^{\mathrm{ur}}/K), H)|}{\sum_{D\leq B} |E_\Gamma(D)|} = ?$$

Let $\mathcal{C}$ be a finite set of finite groups.

Let $G^{\mathcal{C}}$ be the pro-$\mathcal{C}$ completion of G with respect to $\mathcal{C}$.

Characteristic functions

$$\lim_{B\to\infty} \frac{\sum_{D\leq B} |\{K \in E_\Gamma(D) \mid \mathrm{Gal}(K^{\mathrm{ur}}/K)^{\mathcal{C}} \simeq H^{\mathcal{C}}\}|}{\sum_{D\leq B} |E_\Gamma(D)|} = ?$$

Admissible groups

Restrict to $K/\mathbb{Q}$ **totally real**, and $K^{\#} = K^{\mathrm{ur},2|\Gamma|'}$ (prime to $2|\Gamma|$ part).

1. (Γ-group) Γ acts on H continuously.
2. (Admissible) $\mathrm{GCD}(|H|, |\Gamma|) = 1$ and
$$H = \overline{\langle g^{-1}\gamma(g) : g \in H \,|\, \gamma \in \Gamma \rangle}$$
3. (Property E) For all $p \nmid 2|\Gamma|$, for all non-split central Γ-extensions
$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & \widetilde{G} \arrow[r] & G \arrow[r] & 1 \\ & & & H \arrow[u, "\forall\,\mathrm{surj}"'] \arrow[ul, dashed, "\exists"] & \end{tikzcd}$$

Proposition

The group $H = \mathrm{Gal}(K^{\#}/K)$ is admissible, and property E holds.

How to model $\mathrm{Gal}(K^{\#}/K)$?

Let $F_n(\Gamma)$ be the free pro-$|\Gamma|'$-group on $\{x_{i,\gamma} \mid i = 1, \ldots, n \text{ and } \gamma \in \Gamma\}$.

Let $\mathcal{F}_n = \overline{\langle x_{i,\mathrm{id}}^{-1}\gamma(x_{i,\mathrm{id}}) \mid i = 1, \ldots, n\rangle} \subset F_n(\Gamma)$ be the free admissible Γ-group on n generators.

Proposition

A quotient of $\mathcal{F}_n$ has Property E if and only if it is isomorphic to

$$\mathcal{F}_n/[r^{-1}\gamma(r)]_{r\in S,\gamma\in\Gamma}$$

for some $S \subset \mathcal{F}_n$

Definition

We thus define a random group $X_{\Gamma,n} := \mathcal{F}_n/[r^{-1}\gamma(r)]_{r\in S,\gamma\in\Gamma}$, where $(s_1, \ldots, s_{n+1})$ is random from Haar measure on $\mathcal{F}_n^{n+1}$ and $S = \{s_1, \ldots, s_{n+1}\}$.

Main theorem

Theorem

There exists a measure μ_Γ on the set X of isomorphism classes of admissible Γ groups.

Specify the measure on the "basic opens" $U_{\mathcal{C},H} := \{G \mid G^{\mathcal{C}} \simeq H^{\mathcal{C}}\}$.

This measure specializes to the "usual" Cohen–Lenstra measure.

"Conjecture"

$\mathrm{Gal}(K^{\#}/K)$ equidistributes with respect to μ_Γ.

Theorem

This conjecture is true for moments over $\mathbb{F}_q(t)$ as $q \to \infty$.

Main conjecture

Let $E_\Gamma(D)$ be the set of **totally real** Γ-extensions $K/\mathbb{Q}$ with $\operatorname{rDisc} K = D$.

Recall that $K^\# = K^{\mathrm{ur},2|\Gamma|'}$ (prime to $2|\Gamma|$ part).

Let H be an admissible profinite group.

Moments

$$\lim_{B\to\infty} \frac{\sum_{D\le B}\sum_{K\in E_\Gamma(D)} |\operatorname{Sur}_\Gamma(\operatorname{Gal}(K^\#/K),H)|}{\sum_{D\le B}|E_\Gamma(D)|} = \int_X |\operatorname{Sur}_\Gamma(X,H)|\, d\mu_\Gamma(X)$$

$$= [H : H^\Gamma]^{-1}$$

Let $\mathcal{C}$ be a finite set of finite Γ-groups, each with order coprime to $2|\Gamma|$.

Characteristic Functions

$$\lim_{B\to\infty} \frac{\sum_{D\le B} |\{K\in E_\Gamma(D) \mid \operatorname{Gal}(K^\#/K)^{\mathcal{C}} \simeq H^{\mathcal{C}}\}|}{\sum_{D\le B}|E_\Gamma(D)|} = \mu_\Gamma(U_{\mathcal{C},H})$$

Function fields: $\mathbb{F}_q(t) \subset \mathbb{F}_q(C)$

$$
\begin{array}{ccccc}
K & \qquad & \mathbb{F}_q(C) & \qquad & C \\
\Big| & & \Big| & & \Big\downarrow \\
\mathbb{Q} & & \mathbb{F}_q(t) & & \mathbb{P}^1
\end{array}
$$

Function fields: $\mathbb{F}_q(t) \subset \mathbb{F}_q(C)$

More Geometry

$$\mathrm{Cl}(K) = \mathrm{Pic}(\mathrm{Spec}\,\mathcal{O}_K)$$

VS

$$0 \to \mathrm{Pic}^0(C) \to \mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Function fields: $\mathbb{F}_q(t) \subset \mathbb{F}_q(C)$

More Geometry

$$\mathrm{Cl}(K) = \mathrm{Pic}(\mathrm{Spec}\,\mathcal{O}_K)$$

VS

$$0 \to \mathrm{Pic}^0(C) \to \mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Different tools: $\mathrm{Jac}_C = \mathrm{Pic}^0(C)$

$$\mathrm{Frob} \in \mathrm{Gal}_{\mathbb{F}_q} \to \mathrm{Aut}\, T_\ell(\mathrm{Jac}_C) \cong \mathbb{Z}_\ell^{2g}$$

$$\mathrm{coker}\,(\mathrm{Frob} - \mathrm{Id}) \cong \mathrm{Jac}_C(\mathbb{F}_q)_\ell = \mathrm{Pic}^0(C)_\ell$$

Weil conjectures

Let X be an algebraic variety over $\mathbb{Z}_p$.

Trace formula

$X(\mathbb{F}_p) = X(\overline{\mathbb{F}_p})^{\mathrm{Frob}} = \sum_{i=0}^{\infty}(-1)^i \operatorname{Tr} \mathrm{Frob}\,|H^i_{\text{ét},c}(X_{\mathbb{F}_p}, \overline{\mathbb{Q}}_\ell)$

Weil cohomology

$H^i_{\text{ét},c}(X_{\mathbb{F}_p}, \overline{\mathbb{Q}}_\ell) = H^i_{\mathrm{sing}}(X(\mathbb{C}), \overline{\mathbb{Q}}_\ell)$

Geometric analytic number theory

Idea

Use algebraic topology (over $\mathbb{C}$) to prove analytic theorems over $\mathbb{F}_p$.

Example (Ellenberg, AWS)

1. Let $\mathrm{sf}_k(n)$ be the set of squarefree monic polynomials in $k[x]$ of degree n.
2. Exercise: $\#\,\mathrm{sf}_{\mathbb{F}_q}(n) = q^n - q^{n-1}$.
3. Note:
$$\frac{\#\,\mathrm{sf}_{\mathbb{F}_q}(n)}{q^n} = 1 - \frac{1}{q} = \zeta_{\mathbb{A}^1_{\mathbb{F}_q}}(2)^{-1}$$

Configuration space

1. $\mathrm{Conf}_n X = (X^n - \Delta)/S_n$
2. $(\mathrm{Conf}_n \mathbb{A}^1)(k) \cong \mathrm{sf}_k(n)$
3. $\{\alpha_1, \ldots, \alpha_n\} \mapsto (x - \alpha_1) \cdots (x - \alpha_n)$
4. $\pi_1(\mathrm{Conf}_n(\mathbb{C})) = B_n$ (Braid group)

Theorem (Arnol'd)

$$H^i(\mathrm{Conf}_n(\mathbb{C}); \mathbb{Q}) = \begin{cases} \mathbb{Q} & \textit{if } i = 0, 1 \\ 0 & \textit{if } i > 1 \end{cases}$$

$$\sum_{i=0}^{\infty} (-1)^i \operatorname{Tr} \mathrm{Frob} \,|\, H^i_{\text{ét},c}(X, \overline{\mathbb{Q}}_\ell) = \operatorname{Tr} \mathrm{Frob} \,|\, H^0 - \operatorname{Tr} \mathrm{Frob} \,|\, H^1 = q^n - q^{n-1}$$

Hurwitz spaces

$$
\begin{array}{ccc}
(C \xrightarrow{f} \mathbb{P}^1, \iota\colon G \cong \operatorname{Aut} f) & \qquad & \mathrm{Hur}^n_{G,c} \\
\downarrow & & \downarrow \\
\Delta_f & & \mathrm{Conf}_n(\mathbb{P}^1)
\end{array}
$$

1. f is a **tamely ramified** G **cover**
2. with n **ramified points**
3. with an **unramified marked point at infinity**

4. c is a **multiset of conjugacy classes** of **cyclic subgroups** of G
5. $\mathrm{Hur}_{G,c}$ consists of **covers whose inertia agrees** with c.

Main point

Let H be a finite Γ-admissible group with order coprime to $2|\Gamma|q(q-1)$

1. Let $Q = \mathbb{F}_q(t)$.
2. $G = H \rtimes \Gamma$
3. $\coprod_c \mathrm{Hur}^n_{G,c}(\mathbb{F}_q) \cong \{\text{surjections } \mathrm{Gal}(\overline{Q}/Q) \to H \rtimes \Gamma\}$

Theorem (Liu–Wood–ZB)

We can compute components of $\mathrm{Hur}^n_{G,c}$ *"topologically".*

In particular, over $\mathbb{F}_q(t)$ we can prove our conjecture for moments as

$$q \to \infty \text{ with } (q, |\Gamma||H|) = 1, (q-1, |H|) = 1.$$

This abelianizes to (suitably modified) versions of the Cohen–Lenstra–Martinet heuristics

Main theorem (over function fields)

Let $E_\Gamma(D, \mathbb{F}_q(t))$ denote the set of isomorphism classes of totally real Γ-extensions K of $\mathbb{F}_q(t)$ such that $\operatorname{rDisc} K = D$.

Theorem (Liu–Wood–ZB)

Let H be a finite admissible Γ-group. Then,

$$\lim_{N\to\infty} \lim_{\substack{q\to\infty \\ (q,|\Gamma||H|)=1 \\ (q-1,|H|)=1}} \frac{\sum_{n\leq N} \sum_{K\in E_\Gamma(q^n,\mathbb{F}_q(t))} \left|\operatorname{surj}_\Gamma(\operatorname{Gal}(K^\#/K), H)\right|}{\sum_{n\leq N} |E_\Gamma(q^n, \mathbb{F}_q(t))|}$$

$$= \int_X |\operatorname{surj}_\Gamma(X, H)| d\mu_\Gamma(X) = [H : H^\Gamma]^{-1}$$

$$\# \operatorname{Hur}^n_{G,c}(\mathbb{F}_p) = \operatorname{Tr}\operatorname{Frob} | H^0_c(\operatorname{Hur}^n_{G,c}) - \operatorname{Tr}\operatorname{Frob} | H^1_c(\operatorname{Hur}^n_{G,c}) \ldots$$