1

ISTA, Klosterneuburg,
05/12/2024

Asymptotic distribution of wildly ramified extensions of function fields

I) Brief history

- Maybe the story begins with inverse Galois theory, studied since the late XIXth century (Hilbert, Noether):
  ? Is every finite group the Galois group of an extension of $\mathbb{Q}$?

- Inverse problems can be made quantitative:

$$N_{K,G}(X) := \left| \left\{ \begin{array}{c} \text{Galois extensions} \\ L|K \end{array} \middle| \begin{array}{c} Gal(L|K) \simeq G \\ \|\mathrm{Disc}(L|K)\| \leq X \end{array} \right\} \right|.$$

Theorem (Mäki over $\mathbb{Q}$, Wright in general; 1985-89):
If G is abelian, K a global field with char $K \nmid |G|$, then:

$$N_{K,G}(X) \underset{X \to +\infty}{\sim} C\, X^{1/a} (\log X)^{b-1}$$

where $C > 0$, u smallest prime factor of $|G|$, $a = |G|(1-\frac{1}{u})$, $b = \frac{|G[u]|}{[K(\zeta_u):K]}$

What about non-abelian groups? When K is a number field:

Conjecture (Malle(*), 2002): for all $\varepsilon > 0$, there are $0 < C_1 \leq C_2$ s.t.

$$C_1 X^{1/a} \leq N_{K,G}(X) \leq C_2 X^{1/a+\varepsilon}$$

with a explicit.

(Over $\mathbb{Q}$, the lower bound $1 \leq \ldots$ for $X >> 1$ is the inverse Galois pb.)

(*) There is a strong version of the conjecture, but it is known to be false.

▶ Over the rational function field $K := \mathbb{F}_q(T)$, when $\underbrace{\gcd(q, |G|) = 1}_{\text{only tame ramification}}$, the upper bound in Malle's conjecture was proved by Ellenberg–Tran–Westerland in 2023.

$$\left\{\begin{matrix}G\text{-extensions of } K\\ \text{disc.} \leq n\end{matrix}\right\} \simeq \left\{\begin{matrix}G\text{-covers of } \mathbb{P}^1_K\\ \underline{\deg(\text{branch locus})} \leq n\end{matrix}\right\} \simeq \left\{\begin{matrix}\mathbb{F}_q\text{-points of the moduli}\\ \text{space } \mathrm{Hur}_{G,n} \text{ of tamely}\\ \text{ramified covers of } \mathbb{P}^1\\ \text{with } n \text{ branch points}\end{matrix}\right\}$$

equivalence smooth curves || function fields

should be weighted by the orders of monodromy elements

there are problems when the moduli space is coarse.

⤳ Estimate $|\mathrm{Hur}_{G,n}(\mathbb{F}_q)|$ (= fixed points of Frobenius!) when $n \to +\infty$. Grothendieck–Lefschetz's trace formula reduces this (for q large) to algebraic topology (cohomology computations).

▶ The wild case is largely unexplored.

⤳ even locally, the problem is interesting.

⤳ the ramification filtration plays a central role.

We will focus on p-groups (no tame ramification at all! ⊛)

Results when G is <u>abelian</u>:

- asymptotics when counting locally by discriminant (Lagemann 2010)
- " globally by conductor (Lagemann 2012, 2015)
- " locally by conductor (Klüners–Müller 2020)
- " locally & globally by discriminant if $G = (\mathbb{Z}/p\mathbb{Z})^r$ (Potthast 2024)

<u>Methods</u>: · class field theory (Artin–Schreier–Witt)

· analytic tools (Dirichlet series & Tauberian theorems)

Our goal: deal with some non-abelian groups.

⊛ In the "mixed" case, everything is complicated even over $\mathbb{F}_p(T)$ (geometrically).
cf. Abhyankar's conjecture.

③

II Parametrization of extensions

1. GENERAL PRINCIPLE

F a field; $\Gamma_F := \mathrm{Gal}(F^{sep}|F)$.

Rk: "G-extensions of F" include étale F-algebras.

$$\{G\text{-extensions of } F\} \xleftrightarrow{\sim} H^1(\Gamma_F, G) = \mathrm{Hom}(\Gamma_F, G)/\text{conjugacy}.$$

Theorem A: Let $G_{F^{sep}}$ be a group equipped with a Γ_F-action and a Γ_F-equivariant group homomorphism $\sigma : G_{F^{sep}} \to G_{F^{sep}}$.
Let $G_F = G_{F^{sep}}^{\Gamma_F}$ and $G = G_{F^{sep}}^{\sigma}$ (fixed points of σ).
Assume:
(i) $G \subseteq G_F$
(ii) The map $\wp : \begin{cases} G_{F^{sep}} \to G_{F^{sep}} \\ g \mapsto \sigma(g)g^{-1} \end{cases}$ is surjective.
(iii) $H^1(\Gamma_F, G_{F^{sep}}) = \{1\}$ (cohomology pointed set)
Then, there is a bijection:

$$\underbrace{H^1(\Gamma_F, G)}_{G\text{-extensions of } F} \xleftrightarrow{\sim} \underbrace{G_F /\!/ G_F}_{\text{orbits of } G_F \text{ acting on itself via } g\cdot m = \sigma(g)\, m\, g^{-1}}.$$

Idea: Let $\gamma : \Gamma_F \to G$. Then:
- $H^1(\Gamma_F, G_{F^{sep}}) = \{1\} \Longrightarrow \exists g \in G_{F^{sep}},\ \gamma(\tau) = g^{-1}\tau(g)$.
- γ is valued in $G \Longrightarrow \wp(g) \in G_F$.

The bijection then maps $[\gamma]$ to $[\wp(g)]$.
(Details left as exercise. Surjectivity uses (ii).)

The typical situation is when F has characteristic p, and $G_{F^{sep}} = \mathcal{G}(F^{sep})$ for some algebraic group $\mathcal{G}$ over $\mathbb{F}_p$, then $G_F = \mathcal{G}(F)$, $G = \mathcal{G}(\mathbb{F}_p)$.

④

Examples: Let F be a field of characteristic p.

- $G_{F^{sep}} = F^{sep}$, $G_F = F$, $G = \mathbb{Z}/p\mathbb{Z}$.
  We obtain: $H^1(\Gamma_F, \mathbb{Z}/p\mathbb{Z}) \simeq F/\wp(F)$ $\longrightarrow$ Artin-Schreier theory.

- V = finite $\mathbb{Z}_p$-module (i.e., any finite abelian p-group)
  $G_{F^{sep}} = V \otimes_{\mathbb{Z}_p} W(F^{sep})$, $G_F = V \otimes_{\mathbb{Z}_p} W(F)$, $G = V$.
  We obtain: $H^1(\Gamma_F, V) \simeq V\otimes W(F) / \wp(V \otimes W(F))$ $\longrightarrow$ (a form of) Artin-Schreier-Witt theory.

A non-abelian example:

- $G_{F^{sep}} = GL_n(F^{sep})$, $G_F = GL_n(F)$, $G = GL_n(\mathbb{F}_p)$.
  We obtain: $\underbrace{H^1(\Gamma_F, GL_n(\mathbb{F}_p))}_{\text{n-dimensional Galois representations mod } p} \simeq \underbrace{GL_n(F) // GL_n(F)}_{\text{iso. classes of n-dim. F-vector spaces equipped with a } \sigma\text{-linear map } \varphi}$

étale φ-modules

2. p-GROUPS OF NILPOTENCY CLASS ≤ 2 ⊛

Let p be an odd prime and G be a finite p-group of nilpotency class ≤ 2, i.e., $[G,G] \subseteq Z(G)$.

- We can equip G with a different group law: $x+y := xy[x,y]^{-1/2}$ (G is uniquely 2-divisible)
  The law $+$ is abelian $\rightsquigarrow$ we denote by $\mathfrak{g}$ the $\mathbb{Z}_p$-module $(G,+)$.
  The commutator $[-,-] : \mathfrak{g}^2 \to \mathfrak{g}$ is alternating, $\mathbb{Z}_p$-bilinear. (Jacobi's identity is trivial in nilp. class ≤ 2)
  $\rightsquigarrow$ A Lie bracket! $\mathfrak{g}$ is a (finite) Lie $\mathbb{Z}_p$-algebra.

⊛ The principle illustrated here generalizes to p-groups of nilpotency class $< p$. (Lazard correspondence)

⑤

- Conversely, if $\mathfrak{g}$ is a Lie $\mathbb{Z}_p$-algebra, we can turn it into a group by equipping it with the law $\circ$: $x \circ y := x + y + \frac{1}{2}[x,y]$.
  ⤳ A correspondance between Lie $\mathbb{Z}_p$-algebras and p-groups.

- This correspondance respects centers ($Z(G) = Z(\mathfrak{g})$), $\{x \in \mathfrak{g} \mid [x,-]=0\}$
  short exact sequences, ...
  We can think about Lie algebras instead of p-groups.

- What have we gained? We can extend scalars!

$$G \xrightarrow[\text{Lie alg.}]{\text{turn into}} \mathfrak{g} \xrightarrow{\otimes_{\mathbb{Z}_p} W(F^{sep})} \mathfrak{g} \otimes W(F^{sep}) \xrightarrow[\text{group}]{\text{turn into}} \underbrace{(\mathfrak{g} \otimes W(F^{sep}), \circ)}_{\text{natural candidate to apply theorem A to}}.$$

Proposition: The hypotheses of Theorem A are satisfied.

Idea:
- The case $\mathfrak{g} = \mathbb{Z}/p\mathbb{Z}$ essentially amounts to Artin-Schreier theory (▲)
- The general case follows by induction on $|\mathfrak{g}|$: pick a subalgebra $\mathfrak{n} \leq Z(\mathfrak{g})$ isomorphic to $\mathbb{Z}/p\mathbb{Z}$, use the exact sequence $1 \longrightarrow \underbrace{W(F^{sep})/p}_{(▲)} \longrightarrow G_{F^{sep}} \longrightarrow \underbrace{((\mathfrak{g}/\mathfrak{n}) \otimes W(F^{sep}), \circ)}_{\text{induction hypothesis}} \to 1$

Thus:

Theorem B:

$$\underbrace{H^1(\Gamma_F, G)}_{G\text{-extensions of } F} \xleftrightarrow{\sim} \underbrace{\mathfrak{g} \otimes_{\mathbb{Z}_p} W(F) \big/\!\!\big/ (\mathfrak{g} \otimes W(F), \circ)}_{\substack{\text{orbits for the action} \\ g \cdot m = \sigma(g) \circ m \circ (-g)}}$$

From now on:
→ F is a local field: $F = \mathbb{F}_q((\pi))$.
→ The global case follows from a local-global principle & analytic args.
(the parametrization is natural in F.)

6

3. Quasi-fundamental domain

$F = \mathbb{F}_q((\pi))$, $\tilde{\pi} = (\pi, 0, 0, \dots) \in W(F)$, $\mathcal{D}^0 = \left\{ D_0 + \sum_{a \in \mathbb{N} \setminus p\mathbb{N}} D_a \tilde{\pi}^{-a} \;\middle|\; D_a \in W(\mathbb{F}_q) \right\}$.
(Teichmüller representative)

Facts:
- every orbit in $\mathfrak{g} \otimes W(F) /\!/ (\mathfrak{g} \otimes W(F), \circ)$ intersects $\mathfrak{g} \otimes \mathcal{D}^0$.
- if $g \in \mathfrak{g} \otimes W(F)$, $m \in \mathfrak{g} \otimes \mathcal{D}^0$, then:
  $g \cdot m \in \mathfrak{g} \otimes \mathcal{D}^0 \iff g \in \mathfrak{g} \otimes W(\mathbb{F}_q)$.

Thus Theorem B can be made more precise:

Theorem B':

$$H^1(\Gamma_F, G) \xleftrightarrow{\sim} \mathfrak{g} \otimes W(F) /\!/ (\mathfrak{g} \otimes W(F), \circ) \xLeftrightarrow{\sim} \underbrace{\mathfrak{g} \otimes \mathcal{D}^0 /\!/ (\mathfrak{g} \otimes W(\mathbb{F}_q), \circ)}_{\text{much smaller}}$$

+ the acting group $(\mathfrak{g} \otimes W(\mathbb{F}_q), \circ)$ is finite.

{Using a decomposition $\mathfrak{g} \simeq \prod \mathbb{Z}/p^{m_i}\mathbb{Z}$ as a $\mathbb{Z}_p$-module, and coordinates, this already has a "moduli space interpretation": G-extensions of F are parametrized by the ind-scheme $\bigcup_n \mathbb{A}^n_{\mathbb{F}_p}$, up to the action of a finite group.}

From now on:

→ We identify G-extensions of F with orbits $[D]$ of elements of $\mathfrak{g} \otimes \mathcal{D}^0$, under the action of the finite group $(\mathfrak{g} \otimes W(\mathbb{F}_q), \circ)$.

Remark: Parametrizing G-extensions of local fields is not magical: we have a description of their absolute Galois groups as abstract groups (Koch 1967)! However, the ramification filtration is lost in that description.

... Not here!

III Control of higher ramification

Definition: if $D \in \mathfrak{g} \otimes \mathfrak{D}^0$ corresponds to $[\gamma] \in H^1(\Gamma_F, G)$,
we define: $lj(D) := \inf\{ v > 0 \mid \gamma(\underbrace{\Gamma_F^v}) = 1 \}$
"last jump"
v-th ramification subgroup, in the upper numbering.

- $lj(D) \in \frac{1}{|G|}\mathbb{N}$ (if G abelian: $\in \mathbb{N}$ by Hasse–Arf).
- $lj(D) = 0 \iff$ tamely ramified $\underset{\text{(here)}}{\iff}$ unramified!

Theorem (consequence of Abrashkin's work, 1998):
Let $D = D_0 + \sum_{b \in \mathbb{N} \setminus p\mathbb{N}} D_b \tilde{\pi}^{-b}$, $D_b \in \mathfrak{g} \otimes W(\mathbb{F}_q)$.

Let $v > 0$. We define $\mu_v(b) := \min\{ k \in \mathbb{N}_{\geq 0} \mid bp^k \geq v \}$.
Then:

$$\boxed{lj(D) < v \iff \forall b \in \mathbb{N} \setminus p\mathbb{N}, \text{ equations (E1) and (E2) hold}}$$

(E1): $$b p^{\mu_v(b)} \sigma^{\mu_v(b)}(D_b) = -\frac{1}{2} \sum_{n=0}^{\mu_v(b)} p^n \sigma^n \sum_{\substack{a_1 + a_2 = bp^{\mu_v(b)-n} \\ a_1, a_2 < vp^{-n}}} [a_1 D_{a_1}, D_{a_2}]$$
$$- \sum_{n > \mu_v(b)} p^n \sum_{\substack{a_1 p^{n-\mu_v(b)} + a_2 = b \\ a_1, a_2 < vp^{-n}}} [a_1 \sigma^n(D_{a_1}), \sigma^{\mu_v(b)}(D_{a_2})]$$

(E2): for every $m > 0$ such that $b \geq vp^m$:
$$0 = \sum_{n \geq 0} p^n \sum_{\substack{a_1 p^{n+m} + a_2 = b \\ a_1, a_2 < vp^{-n}}} [a_1 \sigma^m(D_{a_1}), D_{a_2}].$$

($p \nmid a_1, a_2$ everywhere)

⑧

Remarks:

(o) These are <u>not</u> polynomial equations over $W(\mathbb{F}_q)$ because of "σ".
These are "difference equations" over $(W(\mathbb{F}_q), \sigma)$.
They can also be seen as polynomial equations over $\mathbb{F}_q$.
(in terms of coordinates of Witt vectors, and replacing σ by the p-th power.)

(i) $lj(D)$ does not depend on D_0! (D_0 appears in neither equation!)
$\rightsquigarrow$ We define $\mathcal{D} = \mathcal{D}^0 / \mathfrak{g} \otimes W(\mathbb{F}_q)$, $\mathrm{pr}: \mathcal{D}^0 \twoheadrightarrow \mathcal{D}$ the canonical projection.

Then $lj(D)$ is well-defined for $D \in \mathcal{D}$.

(ii) $p^{\mu_v(b)} D_b$ belongs to $[\mathfrak{g}, \mathfrak{g}] \otimes W(\mathbb{F}_q) \subseteq Z(\mathfrak{g}) \otimes W(\mathbb{F}_q)$ (cf. (E1))

(iii) $p^{\mu_v(b)} D_b$ is a p-torsion element (express $p^{\mu_v(b)+1} \sigma^{\mu_v(b)} D_b$ using (E1): all terms vanish because of point (ii))

(iv) $D_b = 0$ if $b \geq 2v$ (the sum in (E1) is empty)

Consequences for counting:

$$\sum_{\substack{K|F\text{: } G\text{-extension} \\ lj(K|F) = n}} \frac{1}{|\mathrm{Aut}_F(K)|} = \sum_{\substack{[D] \in \mathfrak{g} \otimes \mathcal{D}^0 /\!/ (\mathfrak{g} \otimes W(\mathbb{F}_q), \circ) \\ lj([D]) = n}} \frac{1}{|\mathrm{Stab}_{(\mathfrak{g} \otimes W(\mathbb{F}_q), \circ)}(D)|}$$

$$= \sum_{\substack{D \in \mathfrak{g} \otimes \mathcal{D}^0 \\ lj(D) = n}} \frac{1}{|\mathfrak{g} \otimes W(\mathbb{F}_q)|} = |\{D \in \mathfrak{g} \otimes \mathcal{D} \mid lj(D) = n\}|.$$

$\rightsquigarrow$ Our goal is then to count $|\{D \in \mathfrak{g} \otimes \mathcal{D} \mid lj(D) < v\}|$.

Remark (iv) gives a first upper bound (a very rough one!):
$$|\{D \in \mathfrak{g} \otimes \mathcal{D} \mid lj(D) < v\}| \leq |\mathfrak{g} \otimes W(\mathbb{F}_q)|^{2v}.$$

Our goal: improve this bound.

IV *Mildly wildly ramified extensions*

(↳ globally, these extensions are the ones that "control" the asymptotics, as most places will not ramify too "deeply")

Let $v \leq p$. Then $\mu_v(b) = \begin{cases} 1 & \text{if } b < v \\ 0 & \text{if } b \geq v. \end{cases}$

This forces $n = 0$ in (E1):

$$b<p \quad \left[\, bp\,\sigma(D_b) = -\frac{1}{2} \sum_{\substack{a_1+a_2=bp \\ a_1,a_2<v}} [a_1 D_{a_1}, D_{a_2}]\right.$$

$$b\geq p \quad \left[\, bD_b = -\frac{1}{2} \sum_{\substack{a_1+a_2<b \\ a_1,a_2<v}} [a_1 D_{a_1}, D_{a_2}]\right.$$

and in (E2) there is at most one term in the sum so:

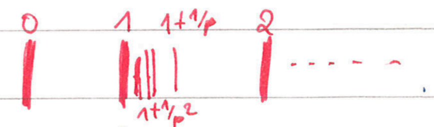
$$(\text{E2}') \quad [\sigma^m(D_{a_1}), D_{a_2}] = 0 \quad \forall \begin{cases} 1 \leq a_1, a_2 < v \\ m > 0 \end{cases} \text{ s.t. } a_1 + a_2 p^{-m} \geq v.$$

$\boxed{v=1} \to \mathrm{lj}(D) < 1 \iff D_b = 0 \ \forall b \in \mathbb{N} \setminus p\mathbb{N} \iff \mathrm{lj}(D) = 0.$

$\boxed{1<v<2} \to$ "$a_1, a_2 < v$" means $a_1 = a_2 = 1$. In particular $[D_{a_1}, D_{a_2}] = 0$.

So: $(\text{E1}) \iff \underbrace{pD_1 = 0}_{b=1}, \quad \underbrace{D_b = 0}_{b \geq 2}.$

$(\text{E2}') \iff [\sigma^m D_1, D_1] = 0 \quad \forall m \text{ s.t. } 1 + p^{-m} \geq v.$

Conclusions: • the possible last jumps look something like 

• The distribution only depends on the p-torsion $\mathfrak{g}[p]$ (a $\mathbb{F}_p$-vector space whose dimension we denote by r.) $r := \dim_{\mathbb{F}_p} \mathfrak{g}[p]$.

• Number of elements of $\mathfrak{g}[p] \otimes_{\mathbb{F}_p} \mathbb{F}_q$ which commute with their Frobenius, Frobenius-squared, etc. . . . ?

Geometric viewpoint: $C := \{x, y \mid [x,y] = 0\}$ defines a closed subvariety of $(\mathbb{A}^r_{\mathbb{F}_p})^2$.

$\Gamma_i = \{x, y \mid y = \sigma^i(x)\}$ graph of σ^i. Can we count $\Big|\underbrace{(\Gamma_0 \times_{\mathbb{A}^r} C \times \cdots \times_{\mathbb{A}^r} C) \cap (\Gamma_1 \times_{\mathbb{A}^r} \Gamma_1 \times_{\mathbb{A}^r} \cdots \times_{\mathbb{A}^r} \Gamma_m)}_{\subseteq (\mathbb{A}^r)^{m+2}}\Big|$ using the trace formula / purity? (cf. Hrushovski-Lang-Weil)

V) Deeply wildly ramified extensions

(↳ for the global counting, we only need upper bounds)

$\mathbb{J}_v$ = closed subvariety of $\mathbb{A}^{\omega}_{\mathbb{F}_p}$ defined by equations (E1), (E2).
(Remark (iv) $\Rightarrow$ $\mathbb{J}_v$ embeds into finite dimensional affine space.)

$$\mathbb{J}_v(\mathbb{F}_q) \approx \left\{ \begin{array}{c} G\text{-extensions of } \mathbb{F}_q((T)) \\ \text{with last jump } < v \end{array} \right\}.$$

⤳ $\mathbb{J}_v$ is like a moduli space for G-covers of a "fat point" with bounded last jump. $G \circlearrowright \begin{smallmatrix} x \\ x \\ \bullet \end{smallmatrix}$.

▸ Counting $\mathbb{F}_q$-points of $\mathbb{J}_v$ is our goal.

Proposition 1. If G has exponent p ($\mathfrak{g}$ is a Lie $\mathbb{F}_p$-algebra) then (E1) is "block-triangular": $(D_b)_{b \geq v}$ is determined by $(D_b)_{b<v}$.

$$\Rightarrow |\mathbb{J}_v(\mathbb{F}_q)| \leq q^{r(v-1)}.$$

Proposition 2. The projection of $\mathbb{J}_v$ on coordinates $(D_b)_{b<v}$ is a finite map with degree $\leq |G|^{2(v-1)}$.

$$\Rightarrow |\mathbb{J}_v(\mathbb{F}_q)| \leq |G|^{2(v-1)} q^{r(v-1)}.$$

Idea: interpret (E1) as a rewriting rule (from left to right).
⤳ Some invariant decreases strictly, and there are at most $|G|^{2(v-1)}$ monomials that cannot be rewritten.

Proposition 3. Assume that, for all $n \geq 1$: $Z(\mathfrak{g}) \cap p^n \mathfrak{g} = p^n Z(\mathfrak{g})$.
Then: $|\mathbb{J}_v(\mathbb{F}_q)| \leq q^{r(v-1)}$. (generalizes Prop. 1)

Idea: first fix $(D_b)_{b \in \mathbb{N} \setminus p\mathbb{N}}$ modulo center, then $p^{\mu_v(b)} D_b$ is determined. Count the possible choices!