Let Γ be a finite group, and let H be a finite admissible Γ-group, i.e. $\gcd(\#H, \#\Gamma) = 1$ and H is generated by elements of the form $h^{-1}\gamma(h)$.

Recall 1 (Notation)**.** Write $Q = \mathbb{F}_q(t)$ for some q. For an extension K/Q, we let $K^{\#}$ denote the maximal unramified extension of K of order prime to $|\mu_Q|\,|\Gamma|\,\mathrm{char}(Q)$ that is split completely at places of K over infinity. Let $\mathrm{rDisc}\, K = \mathrm{Nm}\,\mathrm{rad}\,\mathrm{Disc}(K/Q)$.

Product of ramified places when $Q = \mathbb{Q}$

Let $E_\Gamma(D, Q) = \{K/Q \text{ totally real } \Gamma\text{-extension} : \mathrm{rDisc}\, K = D\}$.

Totally real = split completely over ∞

Theorem 2 (Sur-moment in large q limit)**.**

$$\lim_{N\to\infty} \lim_{\substack{q\to\infty \\ (q,|\Gamma||H|)=1 \\ (g-1,|H|)=1}} \frac{\sum_{n\le N}\sum_{K\in E_\Gamma(q^n,\mathbb{F}_q(t))} \left|\mathrm{Sur}_\Gamma(\mathrm{Gal}(K^{\#}/K), H)\right|}{\sum_{n\le N} |E_\Gamma(q^n, \mathbb{F}_q(t))|} = \frac{1}{[H : H^\Gamma]}$$

where in the limit q is always a prime power.

Have everything up to here written on board before talk starts

Let

$$N(H,\Gamma,D,Q) := \#\left\{\varphi \in \mathrm{Sur}\left(\mathrm{Gal}(\overline{Q}/Q), H \rtimes \Gamma\right) \,\middle|\, \begin{array}{c}\mathrm{rDisc}(K_\varphi/Q) = D,\ \ K_\varphi/Q \text{ split completely at } \infty \\ \text{and } K/K^H \text{ everywhere unramified}\end{array}\right\}$$

Then,

$$\sum_{K\in E_\Gamma(D,Q)} \left|\mathrm{Sur}_\Gamma(\mathrm{Gal}(K^{\#}/K), H)\right| = \frac{1}{[H : H^\Gamma]} N(H,\Gamma,D,Q),$$

so to prove theorem, suffices to show

$$\sum_{n\le N} N(H,\Gamma,q^n,\mathbb{F}_q(t)) \sim \sum_{n\le N} \#E_\Gamma(q^n, \mathbb{F}_q(t))$$

as $q \to \infty$ (satisfying necessary coprimality conditions) then $N \to \infty$.

q prime to $|\Gamma|\,|H|$, and $q-1$ prime to $|H|$

Recall 3. For A some group, and $c \subset A$ an appropriate subset, we have a scheme $\mathrm{Hur}^n_{A,c}/\mathbb{Z}[1/|A|]$ parameterizing triples $(X \xrightarrow{f} \mathbb{P}^1, G \xrightarrow{\sim} \mathrm{Aut}(f), P)$ where

- f is a tame Galois cover unramified above ∞ with inertia at each (branch) point generated by an element of c
- $P \in X$ is a point above ∞.

Recall 4. Let $G_1 = H \rtimes \Gamma$ and let $c_1 \subset G_1$ be the set of elements who have the same order in G as their images in Γ. Then, for q relatively prime to $|G|$ and $n \ge 0$,

TODO: Differentiate G and G_1

$$\#\mathrm{Hur}^n_{G_1,c_1}(\mathbb{F}_q) = N(H,\Gamma,q^n,\mathbb{F}_q(t)).$$

Remark 5. One also has

$$\#\mathrm{Hur}^n_{\Gamma,\Gamma\setminus\{1\}}(\mathbb{F}_q) = E_\Gamma(q^n, \mathbb{F}_q(t)).$$

○

Split completely because Galois + exists an $\mathbb{F}_p$-point over ∞

Goal. Let $\pi_{G_1}(q,n)$ denote the number of $\mathrm{Frob} = \mathrm{Frob}_{(\mathrm{Hur}^n_{G_1,c_1})_{\mathbb{F}_q}}$-fixed components of $(\mathrm{Hur}^n_{G_1,c_1})_{\overline{\mathbb{F}}_q}$, and let $\pi_\Gamma(q,n)$ denote the number of Frob-fixed components of $(\mathrm{Hur}^n_{\Gamma,\Gamma\setminus\{1\}})_{\overline{\mathbb{F}}_q}$. Then,

$$\pi_{G_1}(q,n) \sim \pi_\Gamma(g,n).$$

More specifically, if $d_\Gamma(q)$ denotes the number of orbits of non-trivial conjugacy classes of Γ under taking qth powers of elements, then

Ignore this bit

$$\pi_G(q,n) = \pi_\Gamma(q,n) + O_G\left(n^{d_\Gamma(q)-2}\right)$$

and (ignoring congruence subtleties) $\pi_\Gamma(q,n) \geq C_G n^{d_\Gamma(q)-1}$.

e.g. for quadratic extensions, the discriminant is always an even power of q (i.e. n is even)

To count these components, we recall the lifting invariant.

Setup. Consider a finite group G with a chosen subset $c \subset G\setminus\{1\}$ which is closed under conjugation by elements of G and under invertible powers. Also assume c generates G.

$g^n \in c$ if $g \in c$ and $(n, \mathrm{ord}(g)) = 1$

Recall 6. Let

$$U(G,c) = \left\langle [g] : g \in G \,\middle|\, [x][y][x]^{-1} = [xyx^{-1}] \right\rangle \text{ and } K(G,c) := \ker\left(U(G,c) \xrightarrow{[g]\mapsto g} G\right).$$

For $k = \overline{k}$ a field where $\mathrm{char}\, k \nmid |G|$, we let

$$\widehat{\mathbb{Z}}^\times_k := \varprojlim_n \mathbb{Z}/n\mathbb{Z} \text{ and } \widehat{\mathbb{Z}}(1)^\times_k := \varprojlim_n \mu_n(k)$$

with n ranging over integers coprime to $\mathrm{char}\, k$. There is an action $\widehat{\mathbb{Z}}^\times_k \curvearrowright K(G,c)$ so that every component of $(\mathrm{Hur}^n_{G,c})_k$ has a well-defined **lifting invariant**

$$\mathfrak{z} \in K(G,c)\left\langle -1\right\rangle_k := \mathrm{Mor}_{\widehat{\mathbb{Z}}^\times_k}\left(\widehat{\mathbb{Z}}(1)^\times_k, K(G,c)\right).$$

Furthermore, if $k = \overline{\mathbb{F}}_q$ and $\overline{s} \in \mathrm{Hur}^n_{G,c}(\overline{\mathbb{F}}_q)$, then for any $\zeta \in \widehat{\mathbb{Z}}(1)_{\overline{\mathbb{F}}_q}$, one has

$$\mathfrak{z}_{\mathrm{Frob}(\overline{s})}(\zeta) = q^{-1} * \mathfrak{z}_{\overline{s}}(\zeta).$$

Recall there's a map $U(G,c) \to \mathbb{Z}^{c/G}$. Write

Get here in $\leq$ 25 minutes

- $\mathbb{Z}^{c/G}_{\geq M}$ for the subset of elements all of whose coordinates are $\geq M$.
- $\mathbb{Z}^{c/G}_{\equiv q}$ for the subset of elements whose coordinates which are fixed by the automorphism $e_{\overline{x}} \mapsto e_{\overline{x}^q}$ for $\overline{x} \in c/G$ $(x \in c)$.
- $\mathbb{Z}^{c/G}_n$ for the subset of elements with coordinates summing to n.

Use the same subscripts for $K(G,c)$, e.g. write $K(G,c)_{\geq M}\left\langle -1\right\rangle$ for the elements sending a generator to an element of $\mathbb{Z}^{c/G}_{\geq M}$.

Theorem 7. *For $M \gg 0$, one has the following. Let $Y \hookrightarrow (\mathrm{Hur}^n_{G,c})_{\overline{\mathbb{F}}_q}$ be the union of all components with lifting invariant in $K(G,c)_{\geq M}\left\langle -1\right\rangle_{\overline{\mathbb{F}}_q}$. Then, components of Y are in bijection with their lifting invariants.*[1]

Requires topological input. Need to know the components over $\mathbb{C}$, a comparison theorem, and this

[1] $\mathrm{Hur}^n_{G,c}(\mathbb{C})$ components in bijection with B_n-orbits on c^n with product 1 generating G

So we can get our main term by counting Frob-fixed lifting invariants.

Proposition 8. *Let $n \geq 0$ and let q be a prime power with $(q, |G|) = 1$. Let $d_{G,c}(q)$ be the number of orbits of qth powering on the conjugacy classes in c/G, and let $b(G, c, q, n)$ be the number of* Frob*-fixed component invariants in $K(G, c)_{n,\geq 0} \langle -1 \rangle_{\overline{\mathbb{F}}_q}$. Then,*

Coordinates each ≥ 0 and sum to n

$$\pi_{G,c}(q, n) = b(G, c, q, n) + O_G\left(n^{d_{G,c}(q)-2}\right)$$

(and $\pi_{G,c}(q, n) = 0$ if $b(G, c, q, n) = 0$).

Ignore congruence subtleties

Proof. Consider the union Z_q of all components of $(\mathrm{Hur}^n_{G,c})_{\overline{\mathbb{F}}_q}$ with lifting invariant sending a topological generator to an element with image in $\mathbb{Z}^{c/G}_{\equiv q}$ that has some coordinate $< M$. There are $O_G\left(n^{d_G(q)-2}\right)$ choices of $\underline{m} \in \mathbb{Z}^{c/G}_{n,\geq 0,\equiv q}$ with some component $< M$. A theorem of Ellenberg-Venkatesh says that there are $O_G(1)$ components corresponding to each $\underline{m}$, so we win by the previous theorem. ∎

Coordinates constant on each set of conjugacy classes differing by qth powers

M only depends on G, c, not on n. Pick a coordinate, pick a number $< M$, pick $d_G(q) - 2$ numbers $< n$, and then the last number is determined. Get $O(d_G(q)Mn^{d_G(}$

Fact. $b(G, c, q, n)$ grows like $n^{d_G(q)-1}$ (ignoring modulus subtleties)

Let $G_1 = H \rtimes \Gamma$ with c_1 the (nonzero) elements of G that have the same order as their image in Γ, and let $G_2 = \Gamma$ with $c_2 = \Gamma \setminus \{1\}$. We want to show that

$$b(G_1, c_1, q, n) = b(G_2, c_2, q, n).$$

For this, I first need to quote some facts about the group theory of $U(G, c)$.

Fact. There exists a group $\overline{S} \twoheadrightarrow G$ so that $U(G, c) \simeq \overline{S} \times_{G^{\mathrm{ab}}} \mathbb{Z}^{c/G}$, $K(G, c) \simeq \ker(\overline{S} \to G) \times_{G^{\mathrm{ab}}} \mathbb{Z}^{c/G}$, and $(q, \# \ker(\overline{S} \to G)) = 1$.[2] In this language, we can describe the action $\widehat{\mathbb{Z}}^\times_k \curvearrowright K(G, c)$.

In each conjugacy class $\gamma \in c/G$, pick some element x_γ along with a preimage $\widehat{x}_\gamma$ in $\overline{S}$. If $y = g x_\gamma g^{-1}$, for some G, is in the same class, we set $\widehat{y} := \widetilde{g} \widehat{x}_\gamma \widetilde{g}^{-1}$ (independent of choice of g or $\widetilde{g} \in \overline{S}$). For $x \in c$, we define $[x] = (\widehat{x}, e_x) \in U(G, c)$. For $\alpha \in \widehat{\mathbb{Z}}^\times_k$ and $\gamma \in c/G$, we define $w_\alpha(\gamma) := (\widehat{x_\gamma})^{-\alpha} \widehat{x^\alpha_\gamma} \in \ker(\overline{S} \to G)$. This gives

$$\begin{array}{cccc} W_\alpha : & \mathbb{Z}^{c/G} & \longrightarrow & \ker(\overline{S} \to G) \\ & e_\gamma & \longmapsto & w_\alpha(\gamma). \end{array}$$

The action $\widehat{\mathbb{Z}}^\times_k \curvearrowright K(G, c)$ is given by

$$\alpha \star (g, \underline{m}) = (g^\alpha W_\alpha(\underline{m}), \underline{m}^\alpha).$$

(action on $\mathbb{Z}^{c/G}$ comes from action on G by permuting basis elements)

Corollary 9.

$$\begin{aligned} b(G, c, q, n) &= \sum_{\underline{m} \in \ker\left(\mathbb{Z}^{c/G}_{\equiv q, n, \geq 0} \to G^{\mathrm{ab}}\right)} \mathrm{nr}_{q-1}(W_{q^{-1}}(\underline{m})) \\ &= \sum_{h \in \ker(\overline{S}^2 \to G_2)} \mathrm{nr}_{q-1}(h) \# \left\{ \underline{m} \in \ker\left(\mathbb{Z}^{c/G}_{\equiv q, n, \geq 0} \to G^{\mathrm{ab}}\right) : W_{q^{-1}}(\underline{m}) = h \right\} \end{aligned}$$

[2] This kernel is $\mathrm{H}_2(G, c)$, a quotient of $\mathrm{H}_2(G, \mathbb{Z})$

where nr_{q-1} *counts the number of* $(q-1)$*st roots of* $W_{q^{-1}}(\underline{m}) \in \ker(\overline{S} \to G)$*.*

Proof. Fix an element $\zeta \in \widehat{\mathbb{Z}}(1)^{\times}_{\overline{\mathbb{F}}_q}$ and so identify $K(G,c)\langle -1\rangle$ with $K(G,c)$. A lifting invariant $g = (h,\underline{m}) \in \ker(\overline{S} \to G) \times_{G^{\mathrm{ab}}} \mathbb{Z}^{c/G} = K(G,c)$ is Frob-fixed iff

$$(h,\underline{m}) = g = q^{-1} \star g = \left(h^{q^{-1}} W_{q^{-1}}(\underline{m}), \underline{m}^{q^{-1}}\right).$$

Note that $\underline{m} = \underline{m}^{q^{-1}} \iff \underline{m} \in \mathbb{Z}^{c/G}_{\equiv q}$ and

$$h = h^{q^{-1}} W_{q^{-1}}(\underline{m}) \iff h^{q-1} = W_{q^{-1}}(\underline{m})^q,$$

so $\underline{m} \in \mathbb{Z}^{c/G}_{\equiv q}$ with trivial image in G^{ab} has $\mathrm{nr}_{q-1}(W_{q^{-1}}(\underline{m})^q)$ elements $g \in K(G,c)$ mapping to it s.t. $g = q^{-1} \star g$.

Since q is relatively prime to $\ker(\overline{S} \to G)$, we have $\mathrm{nr}_{q-1}(W_{q^{-1}}(\underline{m})^q) = \mathrm{nr}_{q-1}(W_{q^{-1}}(\underline{m}))$ whence the claim. ∎

Theorem 10. $b(G_1, c_1, q, n) = b(G_2, c_2, q, n)$

Proof. We start with some compatibility between $G_1 = H \rtimes \Gamma$ and $G_2 = \Gamma$.

First note that $(h,\gamma) \in c_1$ iff it gives a splitting of the cyclic subgroup generated by $\gamma \in \Gamma$. Since $(\#H, \#\Gamma) = 1$, Schur-Zassenhaus will tell us that any two such splittings are conjugate (and that there always exists such a splitting) so all elements of G_1 over a fixed $\gamma \in c_1$ are conjugate. Thus, $c_1/G_1 \to c_2/G_2$ is a bijection, so $\mathbb{Z}^{c_1/G_1} \xrightarrow{\sim} \mathbb{Z}^{c_2/G_2}$ and so $d_{G_1,c_1}(q) = d_{G_2,c_2}(q)$.

Need $(g^{-1}\gamma(g), \gamma) = (h,\gamma)$ for some $g \in H$

Fact. We can choose groups $\overline{S}^i$ for G_i $(i = 1,2)$ as before so that

$$\begin{tikzcd}
\mathbb{Z}^{c_1/G_1} \arrow[r, "W^1_{q^{-1}}"] \arrow[d, "\simeq"'] & \ker\left(\overline{S}^1 \to G_1\right) \arrow[d, "f"] \\
\mathbb{Z}^{c_2/G_2} \arrow[r, "W^2_{q^{-1}}"] & \ker(\overline{S}^2 \to G_2)
\end{tikzcd}$$

commutes and $(\#\ker(f), q-1) = 1$.

In particular, any element of $\ker(\overline{S}^2 \to G_2)$ has the same number of $(q-1)$st roots as any of its preimages in $\ker(\overline{S}^1 \to G_1)$. Hence,

f surjects onto image of $W^2_{q^{-1}}$ by commutativity

$$\begin{aligned}
b(G_1,c_1,q,n) &= \sum_{\widetilde{h} \in \ker(\overline{S}^1 \to G_1)} \underbrace{\mathrm{nr}_{q-1}(\widetilde{h})}_{\mathrm{nr}_{q-1}(f(\widetilde{h}))} \# \left\{\underline{m} \in \ker\left(\mathbb{Z}^{c_1/G_1}_{\equiv q,n,\geq 0} \to G_1^{\mathrm{ab}}\right) : W^1_{q^{-1}}(\underline{m}) = \widetilde{h}\right\} \\
&= \sum_{h \in \ker(\overline{S}^2 \to G_2)} \mathrm{nr}_{q-1}(h) \# \left\{\underline{m} \in \ker\left(\mathbb{Z}^{c_1/G_1}_{\equiv q,n,\geq 0} \to G_1^{\mathrm{ab}}\right) : W^1_{q^{-1}}(\underline{m}) \in f^{-1}(h)\right\} \\
&= \sum_{h \in \ker(\overline{S}^2 \to G_2)} \mathrm{nr}_{q-1}(h) \# \left\{\underline{m} \in \ker\left(\mathbb{Z}^{c_2/G_2}_{\equiv q,n,\geq 0} \to G_2^{\mathrm{ab}}\right) : W^2_{q^{-1}}(\underline{m}) = h\right\} \\
&= b(G_2,c_2,q,n)
\end{aligned}$$

∎