CONNECTED COMPONENTS OF HURWITZ SCHEMES AND MALLE'S CONJECTURE

SEYFI TÜRKELLI

Abstract. Let $Z(X)$ be the number of degree-$n$ extensions of $F_q(t)$ with some specified Galois group and with discriminant bounded by $X$. The problem of computing the asymptotics for $Z(X)$ can be related to a problem of counting $F_q$-rational points on certain Hurwitz spaces. Ellenberg and Venkatesh used this idea to develop a heuristic for the asymptotic behavior of $Z_0(X)$, the number of -geometrically connected- extensions, and showed that this agrees with the conjectures of Malle for function fields. We extend Ellenberg-Venkatesh’s argument to handle the more complicated case of covers of $P^1$ which may not be geometrically connected, and show that the resulting heuristic suggests a natural modification to Malle’s conjecture which avoids the counterexamples, due to Klüners, to Malle’s conjecture.

1. Introduction

Let $K$ be a number field and let $G \leq S_n$ be a transitive group. Let $S = \text{Stab}_N(1) \subseteq G$ be the stabilizer of $1 \in \{1, ..., n\}$ in $G$. By a $G$-extension, we mean a Galois extension $L/K$ whose Galois group is isomorphic to $G$. We will denote the absolute value $|N^G_K \text{Disc}(L/K)|$ of the norm of the discriminant of a finite extension $L/K$ by $\delta(L/K)$. It is well known that, given a positive number $X$, the number of isomorphism classes of extensions $L/K$ of fixed degree with $\delta(L/K) < X$ is finite. In [17], Malle conjectures an asymptotic formula for the number of isomorphism classes of $G$-extensions $L/K$ of fixed degree with $\delta(L/K) < X$ where $L^S$ is the field fixed by $S$. In order to state Malle’s conjecture precisely, we need to introduce some invariants of the group $G$.

Let $\mathfrak{R}$ be a number field and let $G \leq S_n$ be a transitive group. Let $S = \text{Stab}_N(1) \subseteq G$ be the stabilizer of $1 \in \{1, ..., n\}$ in $G$. By a $G$-extension, we mean a Galois extension $L/\mathfrak{R}$ whose Galois group is isomorphic to $G$. We will denote the absolute value $|N^G_\mathfrak{R} \text{Disc}(L/\mathfrak{R})|$ of the norm of the discriminant of a finite extension $L/\mathfrak{R}$ by $\delta(L/\mathfrak{R})$. It is well known that, given a positive number $X$, the number of isomorphism classes of extensions $L/\mathfrak{R}$ of fixed degree with $\delta(L/\mathfrak{R}) < X$ is finite. In [17], Malle conjectures an asymptotic formula for the number of isomorphism classes of $G$-extensions $L/\mathfrak{R}$ of a fixed number field $\mathfrak{R}$ with $\delta(L^S/\mathfrak{R}) < X$ where $L^S$ is the field fixed by $S$. In order to state Malle’s conjecture precisely, we need to introduce some invariants of the group $G$.

Let $g \in G$. We define the index of $g$ to be the number $\text{ind}(g) = n - r$ where $r$ is the number of orbits of $g$ on the set $\{1, 2, ..., n\}$. Equivalently, $r$ is the number of cycles in cycle decomposition of $g \in S_n$. We define the index of the group $G$, $\text{ind}(G)$, to be the minimum of the set $\{\text{ind}(g) \mid g \in G^\#\}$ where $G^\# = G - \{1\}$. Finally, we define our first invariant $a(G) = 1/\text{ind}(G)$.

Given a conjugacy class $c$ of $G$, its index $\text{ind}(c)$ denotes the index of a representative of the conjugacy class $c$. In order to define our second invariant, we let $C(G)$ be the set of conjugacy classes of $G^\#$ whose index is equal to the index of $G$ (the ones with the minimal index).

Let $\bar{\mathfrak{R}}$ be a separable closure of $\mathfrak{R}$ and $G_{\bar{\mathfrak{R}}}$ denote the absolute Galois group $\text{Gal}(\bar{\mathfrak{R}}/\mathfrak{R})$ of $\mathfrak{R}$. The absolute Galois group $G_{\bar{\mathfrak{R}}}$ acts on the set $C(G)$ via the cyclotomic character as follows: Let $m = |G|$ and $\chi : G_{\bar{\mathfrak{R}}} \rightarrow (\mathbb{Z}/m\mathbb{Z})^*$ be the composition of the cyclotomic character $G_{\bar{\mathfrak{R}}} \rightarrow \hat{\mathbb{Z}}^*$ and the projection $\hat{\mathbb{Z}}^* \rightarrow (\mathbb{Z}/m\mathbb{Z})^*$. If $c \in C(G)$ is the conjugacy class of $g \in G$, then one defines, for $x \in G_{\bar{\mathfrak{R}}}$, the conjugacy class $c^{\chi(x)}$ to be the conjugacy class of $g^{\chi(x)}$.
Now, we define our second invariant to be the number \( b(\mathfrak{K}, G) = |\mathcal{C}(G)/G| \) of \( G_{\mathfrak{K}} \)-orbits on \( \mathcal{C}(G) \).

Fix \( \mathfrak{K} \) and denote the number of isomorphism classes of \( G \)-extensions \( \mathcal{L}/\mathfrak{K} \) with \( \delta(\mathcal{L}^{S}/\mathfrak{K}) < X \) by \( Z_G(\mathfrak{K}, X) \). Malle’s conjecture is stated as follows:

**Conjecture 1.1** (Malle, [17]). Let \( k \) be a number field and \( G \) be a transitive subgroup of \( S_n \). Then,

\[
Z_G(\mathfrak{K}, X) \asymp X^{a(G)}(\log X)^{b(\mathfrak{K},G)-1},
\]

that is, there are positive constants \( A, B \) depending on the base field \( \mathfrak{K} \) and the group \( G \) such that for sufficiently large \( X \) we have

\[
AX^{a(G)}(\log X)^{b(\mathfrak{K},G)-1} < Z_G(\mathfrak{K}, X) < BX^{a(G)}(\log X)^{b(\mathfrak{K},G)-1}.
\]

Note that this conjecture is known for abelian groups and \( \mathfrak{K} = \mathbb{Q} \) by the work of Wright [22], for \( G = S_3 \) by the work of Davenport-Heilbronn [6] and Datskovsky-Wright [8], for \( G = S_4, S_5 \) and \( \mathfrak{K} = \mathbb{Q} \) by the work of Bhargava [1, 2], and for \( G = D_4 \) and \( \mathfrak{K} = \mathbb{Q} \) by the work of Cohen, Diaz y Diaz and Oliver [5]. In [14], Klüners and Malle proved that for each positive \( \epsilon > 0 \) there are positive constants \( c_{\epsilon}, C_{\epsilon} \) such that \( c_{\epsilon}X^{a(G)} < Z_N(\mathbb{Q}, X) < C_{\epsilon}X^{a(G)+\epsilon} \) for any nilpotent group \( G \) given with its regular representation \( G \hookrightarrow S_{|G|} \).

Recently, Klüners gave the following counterexample to this conjecture in [15]: Let \( \mathfrak{K} = \mathbb{Q} \) and \( G = \left( \langle (123) \rangle \oplus \langle (456) \rangle \right) \rtimes \langle (14)(25)(36) \rangle \leq S_6 \). Note that \( G \) is isomorphic to \( C_3 \wr C_2 \) where \( C_r \) is the cyclic group with \( r \) elements. Then, one can easily see that the conjecture predicts that \( Z_N(\mathbb{Q}, X) \asymp X^{1/2} \). Klüners shows that \( Z_G(\mathbb{Q}, X) \asymp X^{1/2} \log X \). He also points out that if one counts only the extensions without an intermediate cyclotomic extension of the base field, then one gets the asymptotic in the conjecture.

### 1.1. The statements of the results

One can state the conjecture for \( \mathfrak{K} = \mathbb{F}_q(t) \) with evident modifications. In this setting, constant intermediate extensions correspond to intermediate cyclotomic extensions. Therefore, regular extensions of \( \mathbb{F}_q(t) \) correspond to the extensions without an intermediate cyclotomic extension. Subject to some heuristics on Hurwitz schemes, Ellenberg and Venkatesh [10] compute the size of the main term in the asymptotic for the number of regular \( G \)-extensions of \( \mathbb{F}_q(t) \), and obtain the analogue of Malle’s conjecture.

This suggests that Malle’s conjecture may correctly predict the asymptotics for extensions without cyclotomic (constant) subextensions. Using the idea of Ellenberg-Venkatesh [10], we will count \( G \)-extensions \( \mathcal{L}/\mathbb{F}_q(t) \) with a maximal constant subextension corresponding to a fixed normal subgroup \( N \); we will call such an extension \( G_N \)-extension and we will let \( Z_{N,G}(\mathbb{F}_q(t), X) \) be the number of \( G_N \)-extensions with discriminant \( < X \). Then, we will take the maximum of \( Z_{N,G}(\mathbb{F}_q(t), X) \) as \( N \) varies to get the asymptotic for \( Z_G(\mathbb{F}_q(t), X) \). We will propose a conjecture eliminating the Klüners’ counterexamples and compatible with the existing results.

The idea is as follows: the category of \( G_N \)-extensions of \( \mathbb{F}_q(t) \) is equivalent to the category of strong \((N,G)\)-covers of \( \mathbb{P}^1_{\mathbb{F}_q} \), see section 2.2 for the definition. Therefore, counting extensions is equivalent to counting \( \mathbb{F}_q \)-rational points on the moduli space of certain covers of \( \mathbb{P}^1 \), namely Hurwitz schemes. Assuming Heuristic 1.3 below for the Hurwitz schemes, we reduce the problem to the one of counting irreducible components of Hurwitz spaces, and computing their dimension.
More precisely, moduli scheme $\mathcal{H}_N/\mathbb{F}_q$ of $N$-covers of $\mathbb{P}^1$ can be written as a disjoint union

$$
\mathcal{H}_N \times \mathbb{F}_q = \bigcup \mathcal{H}_C
$$

of (not necessarily connected, possibly empty) schemes $\mathcal{H}_C$ that are defined a priori over $\mathbb{F}_q$ where the union runs over unordered tuples $\bar{C}$ of conjugacy classes of $N$ of finite length. For a given unordered $k$-tuple $\bar{C} = (C_1, ..., C_k)$ of conjugacy classes of $N$, set $|\bar{C}| := k$ to be the length of the tuple and $r(\bar{C}) := \sum_{i=1}^{k} \text{ind}(C_i)$ where $\text{ind}(C)$ is the index of a representative of the conjugacy class $C$.

Note that the quotient $G/N$ is a cyclic group since it is the Galois group of $\mathbb{F}_{q^d}(t)/\mathbb{F}_q$. Fix a $\tau \in G$ generating the quotient $G/N$. For a given conjugacy class $C$ of $N$, the conjugacy classes $C^g$ and $C^\tau$ denotes the conjugacy classes of $g^\tau$ and $g^\tau$, respectively, where $g$ is any representative of $C$. And, for a given $k$-tuple $\bar{C} = (C_1, ..., C_k)$ of conjugacy classes of $N$, we use the notation: $C^x = (C_1^x, ..., C_k^x)$ for $x = q, \tau$.

For a given integer $e$, we define the cocycle $\zeta_e \in H^1(\mathbb{F}_q, G/N)$ as the one taking $\text{Frob}_q$ to $\tau^e$. Note that the action of the absolute Galois group $G_{\mathbb{F}_q}$ on $G/N$ is trivial so the cocycles are just group homomorphisms. We denote $\zeta_e$-twist of $\mathcal{H}_N$ by $\mathcal{H}^e_N$. We say that such a $k$-tuple $\bar{C} = (C_1, ..., C_k)$ is of $\mathbb{F}_q$-rational of type $e$ if $\tilde{C}^q$ is equal to $\tilde{C}^{\tau^e}$ as an unordered tuple – that is, if they are equal up to a permutation of $C_i$’s. Our motivation for this definition is the following fact, see Theorem 3.2: the component $\mathcal{H}^e_C$ is defined over $\mathbb{F}_q$ if and only if $\bar{C}$ is of $\mathbb{F}_q$-rational of type $e$.

Now, let $\Sigma_{r,e}$ be the set of $\mathbb{F}_q$-rational tuples $\bar{C}$ of type $e$ with $r(\bar{C}) = r$. Notice that the set $\Sigma_{r,e}$ is finite since $N$ is a finite group. Let

$$
h_{cc}(q, r, e) := \sum q^{|\bar{C}|}
$$

where the sum runs over all geometrically connected components of $\mathcal{H}^e_C$’s that are defined over $\mathbb{F}_q$ with $\bar{C} \in \Sigma_{r,e}$. Let $d' := |G/N\text{Cen}_G(N)|$ and

$$
h_{cc}(q, r) := \sum_{\substack{1 \leq e \leq d' \\ (e, d') = 1}} h_{cc}(q, r, e).
$$

Finally, let

$$
\mathcal{Z}_{N,G}'(\mathbb{F}_q, X) = \sum_{q^r < X} h_{cc}(q, r).
$$

Note that, for a given integer $X$, the counting function $\mathcal{Z}_{N,G}'(\mathbb{F}_q, X)$ is just a finite sum of powers of $q$ and that it is intimately related to the connected components of $\mathcal{H}_N$. In general, for a given $k$-tuple $\bar{C}$, it is not true that $\mathcal{H}_\bar{C}$ is connected. In fact, determining the connected components of $\mathcal{H}_N$ is a very old, difficult problem going back to Hurwitz [13]. Our main result gives the asymptotic for this counting function under some conditions.

**Theorem 1.2.** Let $(q, |G|) = 1$. Assume that $G = N \rtimes T$ for some cyclic subgroup $T \subseteq G$ and that $T$ has no nontrivial subgroup that is normal in $G$. Then,

$$
\mathcal{Z}_{N,G}'(\mathbb{F}_q, X) \asymp X^{a(N)(\log X)^{b(N,G,\mathbb{F}_q)-1}}
$$

where $b(N, G, \mathbb{F}_q)$ is an explicitly computable positive integer.
In [10], Ellenberg-Venkatesh uses the following heuristic to get the asymptotics of counting function of $N$-extensions of $\mathbb{F}_q(t)$ that does not contain any nontrivial intermediate constant extension:

**Heuristic 1.3.** Let $\mathcal{H}$ be a geometrically connected scheme of dimension $d$ defined over $\mathbb{F}_q$; then one has $|\mathcal{H}(\mathbb{F}_q)| = q^d$.

We use Heuristic 1.3 and generalize their arguments to relate the counting function $Z'_{N,G}(\mathbb{F}_q, X)$ to the counting function $Z_{N,G}(\mathbb{F}_q(t), X)$ of extensions and get the asymptotics of $G_N$-extensions in Theorem 1.4 below.

Before stating Theorem 1.4, we take a moment to make a couple of remarks about the use of Heuristic 1.3 in our paper (more precisely, in the proof of Lemma 6.2). First of all, we cannot use Lang-Weil bounds since $q$ is fixed in our setting. The heuristic is directly adopted from Ellenberg-Venkatesh [10] and it is only applied to connected components of Hurwitz schemes $\mathcal{H}_g$. We also remark that we do not use the strict equality in Heuristic 1.3 in its full force, which is almost never correct. However, using Theorem 1.2 and the arguments of the paper, one can modify Heuristic 1.3 and obtain the asymptotics in Theorem 1.4. Please see section 6.3 for a detailed remark on the usage of the heuristic in this paper, and a possible modification.

We now describe the result on the counting function $Z_{N,G}(\mathbb{F}_q(t), X)$ more precisely. Let $\mathcal{L}/\mathbb{F}_q(t)$ be a $G$-extension. Let $Z \to \mathbb{P}^1_{\mathbb{F}_q}$ be the corresponding $G$-Galois cover of projective smooth curves. Then, for $C := Z/S$, the cover $C \to \mathbb{P}^1_{\mathbb{F}_q}$ is a degree-$n$ cover. Let $r(\mathcal{L}/\mathbb{F}_q(t))$ be the degree of the ramification divisor\(^1\) of the degree-$n$ cover $C \to \mathbb{P}^1_{\mathbb{F}_q}$. We define our $\delta$-invariant as the integer $\delta(\mathcal{L}/\mathbb{F}_q(t)) := q^{r(\mathcal{L}/\mathbb{F}_q(t))}$, which we will refer to as the discriminant below.

Note that $\delta(\mathcal{L}/\mathbb{F}_q(t))$ is the discriminant of the degree-$n$ extension $\mathcal{L}/\mathcal{L}_{\mathbb{F}_q}(t)$ ($\mathcal{L}_{\mathbb{F}_q}$ is the fixed field of $S$), rather than the one of $\mathcal{L}/\mathbb{F}_q(t)$, where the contribution of the ramification divisor at $\infty$ is also taken into account.

Let $Z_{N,G}(\mathbb{F}_q(t), X)$ be the number of $G_N$-extensions $\mathcal{L}/\mathbb{F}_q(t)$ with $\delta(\mathcal{L}/\mathbb{F}_q(t)) < X$. We will prove the following theorem as a corollary of Theorem 1.2:

**Theorem 1.4.** Let $(q, |G|) = 1$. Assume that $G = N \rtimes T$ for some cyclic subgroup $T \subseteq G$ and that $T$ has no nontrivial subgroup that is normal in $G$. Assume Heuristic 1.3. Then

$$Z_{N,G}(\mathbb{F}_q(t), X) \sim X^{o(N)}(\log X)^{b(N,G,\mathbb{F}_q)-1}$$

where $b(N,G,\mathbb{F}_q)$ is an explicitly computable positive integer.

Note that, in our context, $\mathbb{F}_{q^d}(t)$ is the fixed field of $N$ and so $G/N \cong \text{Gal}(\mathbb{F}_{q^d}(t)/\mathbb{F}_q(t))$. Therefore, the assumption that $T$ is cyclic automatically follows from our setting. But, the assumption that $T$ has no nontrivial subgroup that is normal in $G$ is restrictive; it is equivalent to the condition that, if $\mathcal{L}/\mathbb{F}_q(t)$ is a $G$-extension, the Galois closure of the field $\mathcal{L}^T$

---

\(^1\)Ramification divisor of a branched cover $f : C \to \mathbb{P}^1_{\mathbb{F}_q}$ is defined as follows: For a closed point $P \in C$, let $Q = f(P)$ and $w \in \mathcal{O}_Q$ be a local parameter at $Q$. Consider $w$ as an element of $\mathcal{O}_P$ via the natural map $\mathcal{O}_Q \to \mathcal{O}_P$ induced by $f$. Define the ramification index at $P$ as the integer $e_P = \nu_P(w)$ where $\nu_P$ is the valuation given by $P$ on $\mathcal{O}_P$. Define the degree of the closed point $P$ as the integer $d_P := [\mathbb{F}_q(P) : \mathbb{F}_q]$ where $\mathbb{F}_q(P)$ is the residue field at $P$. Now, the ramification divisor of the degree-$n$ cover $f : C \to \mathbb{P}^1_{\mathbb{F}_q}$ is the divisor $\sum_{P \in C}(e_P - 1)P$ on the curve $C$, and its degree is $\sum_{P \in C}(e_P - 1)d_P$. Here sums run over closed points $P \in C$. 

---
is \( \mathcal{L} \) itself. The splitting assumption that \( G = N \rtimes T \) is also restrictive and does not follow automatically from our setting. For instance, consider the extension of \( \mathbb{F}_5(t) \) generated by the fourth root of \( 2t^2 \). It is a cyclic Galois extension of degree 4 that contains \( \mathbb{F}_{25} \). These assumptions are necessary to use moduli space of \((N,G)\)-covers (in other words, to cite Wewers’ work [21]).

As an immediate consequence of Theorem 1.4, we have the result of Ellenberg and Venkatesh:

**Corollary 1.5.** Assume Heuristic 1.3 and that \( (q, |G|) = 1 \). Then,

\[ Z_{G,G}(\mathbb{F}_q(t), X) \asymp X^{a(G)}(\log X)^{b(G, \mathbb{F}_q) - 1}. \]

In section 4, we will conjecture an asymptotic for the number of \( G \)-extensions of a global field. As evidence in favor of our modification of Malle’s conjecture, we show that our version is not contradicted by Klüners’ counterexample from [15].

**Corollary 1.6.** Assume Heuristic 1.3. Let \( G = ((123)) \oplus ((456)) \rtimes ((14)(25)(36)) \leq S_6 \) and \( q = 2 \mod 3 \) with \( (q, 2) = 1 \). Then, we have

\[ Z_G(\mathbb{F}_q(t), X) \asymp X^{1/2} \log X. \]

We want to count branched covers of \( \mathbb{P}^1_{\mathbb{F}_q} \) corresponding to \( G_N \)-extensions of \( \mathbb{F}_q(t) \), namely strong \((N,G)\)-covers. In section 2, we will give the definitions of the covers in question. These covers are parameterized by certain \( \mathbb{F}_q \)-rational points of Hurwitz schemes of \((N,G)\)-covers of \( \mathbb{P}^1 \). In section 3, we will state well known facts about these moduli schemes. In particular, we will introduce discrete invariants, so called Nielsen tuples, parameterizing “almost” geometrically connected components of Hurwitz schemes and we will determine the components parameterizing strong \((N,G)\)-covers. In section 4, using the heuristic, we will reduce the problem of counting covers to counting Nielsen tuples. In section 5, we prove Theorem 1.4 and we conjecture an asymptotic for \( Z_G(\mathcal{K}, X) \) where \( \mathcal{K} \) is a global field. We give some examples, as corollaries of Theorem 1.4, supporting our conjecture. Finally, we discuss a possible modification of Heuristic 1.3 and its use in our paper.

1.2. The notation. Below, we index the notation used throughout the paper. The definitions of some of the objects below are given in the preceding sections, not here.

- For a given field \( \mathcal{K} \), \( G_{\mathcal{K}} = \text{Gal}(\bar{\mathcal{K}}/\mathcal{K}) \) is the absolute Galois group;
- \( S_n \) is the permutation group of \( \{1, \ldots, n\} \);
- \( G \subseteq S_n \) is a transitive subgroup (on \( n \) letters);
- \( S \subseteq G \) is the stabilizer of \( 1 \in \{1, \ldots, n\} \);
- \( N \subseteq G \) is a normal subgroup of \( G \) and \( T \subseteq G \) is a cyclic subgroup such that \( G = N \rtimes T \) and \( T \) has no nontrivial subgroup that is normal in \( G \);
- \( H := \text{Cen}_G(N) = \{g \in G \mid hg = gh \text{ for all } h \in N\} \);
- \( T' := G/NH \) is the quotient group;
- \( \tau \in T \) a generator of \( T \) and \( \tau_1 \in T' \) is the coset of \( \tau \in T \);
- \( d = |T| \) and \( d' = |T'| \);
- \( \mathcal{H} = \mathcal{H}_{N,G} \) is a coarse moduli scheme for \((N,G)\)-covers (over \( \mathbb{Z}[1/|N|] \));
- \( \mathcal{H}_k = \mathcal{H}_{N,G,k} \) is a coarse moduli scheme for \((N,G)\)-covers with degree \( k \) branch locus (over \( \mathbb{Z}[1/|N|] \));
- \( \mathcal{H}_N \) is a coarse moduli scheme for \( N \)-covers (over \( \mathbb{Z}[1/|N|] \));
- \( q \) is a power of fixed prime such that \( (q, |G|) = 1 \);
- \( \Pi_1(U/\mathbb{F}_q, b) \) is the geometric fundamental group of a scheme \( U/\mathbb{F}_q \);
• $\Pi_1(U/\overline{\mathbb{F}}_q, b)'$ is the maximal pro-prime-to-$q$ quotient of the geometric fundamental group $\Pi_1(U/\overline{\mathbb{F}}_q, b)$.

Acknowledgments. The author is grateful to Jordan Ellenberg for his guidance in preparation of this paper, and thanks to Jürgen Klüners for his very useful comments and pointing out a mistake in an earlier version of the paper. The author also thanks to the referee for helpful comments.

2. $(N,G)$-covers and $N$-Covers

For the rest of the paper, let the notation be as in section 1.2. In this section, first, we will present basic facts about geometric fundamental groups of curves and introduce $(N,G)$-covers of $\mathbb{P}^1$.

2.1. Geometric fundamental groups of curves. In this section, we want to give a brief description of the geometric fundamental groups of curves. For more details of this discussion, see [20]. Let $\mathbb{K}$ be an algebraically closed field.

Let $\mathbb{B}$ be a proper closed reduced subscheme of $\mathbb{P}^1$ of degree $k$ defined over $\mathbb{K}$ and $\mathbb{U} = \mathbb{P}^1 - \mathbb{B}$ be its complement.

In case $\mathbb{K} = \mathbb{C}$, we have a standard presentation of the topological fundamental group $\Pi_{1,\text{top}}(\mathbb{U}(\mathbb{C}), b) = \langle \gamma_1, ..., \gamma_k \mid \gamma_1 \cdots \gamma_k = 1 \rangle$ (1) where $\gamma_i$ is a path going from the base point $b$, encircling a small neighborhood of the $i$-th branch point in positive orientation and coming back to the base point the same way, for a nice picture see [12, p 776]. And, by the Riemann existence theorem, the geometric fundamental group $\Pi_1(\mathbb{U}/\mathbb{C}, b)$ is isomorphic to the profinite completion of the topological fundamental group $\Pi_{1,\text{top}}(\mathbb{U}(\mathbb{C}), b)$. In other words, we have the isomorphism

\[ \Pi_1(\mathbb{U}/\mathbb{C}, b) \cong \hat{\langle \gamma_1, ..., \gamma_k \mid \gamma_1 \cdots \gamma_k = 1 \rangle} \]

where the “widehat” denotes the profinite completion. In fact, this isomorphism is valid for any algebraically closed field $\mathbb{K}$ of characteristic 0.

In case $\mathbb{K} = \mathbb{F}_q$, we don’t have such a simple description of the geometric fundamental group $\Pi_1(U/\overline{\mathbb{F}}_q, b)$. Although the profinite groups $\Pi_1(U/\overline{\mathbb{F}}_q, b)$ and $\Pi_{1,\text{top}}(\mathbb{U}(\mathbb{C}), b)$ are not isomorphic, their prime-to-$q$ parts are isomorphic [20, p 299]. More precisely, denoting the maximal pro-prime-to-$q$ quotient of a profinite group $P$ by $P'$, we have the following description:

\[ \Pi_1(U/\overline{\mathbb{F}}_q, b)' = \langle \gamma_1, ..., \gamma_k \mid \gamma_1 \cdots \gamma_k = 1 \rangle' \]

where $\gamma_i$ corresponds to a generator of an inertia subgroup of $\Pi_1(U/\overline{\mathbb{F}}_q, b)$ at a point of $B$.

Say a morphism $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b) \to N$ is given. Since $(q, |N|) = 1$, the map $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b) \to N$ factors through the projection $pr : \Pi_1(U/\overline{\mathbb{F}}_q, b) \to \Pi_1(U/\overline{\mathbb{F}}_q, b)'$. In other words, there exists a morphism $\phi' : \Pi_1(U/\overline{\mathbb{F}}_q, b)' \to N$ such that $\phi = \phi' \circ pr$. Therefore, any given map $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b) \to N$ is determined by $\phi'(\gamma_1), ..., \phi'(\gamma_k)$.

In order to simplify the formulas below, we abuse the notation and we let $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b)' \to N$ to be the map induced by $\phi$. 
2.2. \((N, G)\)-covers and Strong \((N, G)\)-covers. Recall that we want to count \(G\)-extensions \(\mathcal{L}/\mathbb{F}_q(t)\) containing a certain constant subextension \(\mathbb{F}_{q^d}(t)/\mathbb{F}_q(t)\). We call these extensions \(G_N\)-extensions and define them precisely as follows:

**Definition 2.1.** A \(G_N\)-extension of \(\mathbb{F}_q(t)\) is a \(G\)-extension \(\mathcal{L}/\mathbb{F}_q(t)\) such that \(\mathcal{L}^N/\mathbb{F}_q(t)\) is the maximal constant subextension of \(\mathcal{L}/\mathbb{F}_q(t)\) where \(\mathcal{L}^N\) denotes the subfield of \(\mathcal{L}\) fixed by \(N\).

Note that, by our assumption, \(T\) has no nontrivial subgroup that is normal in \(G\). This implies, if \(\mathcal{L}/\mathbb{F}_q(t)\) is a \(G_N\)-extension, that the Galois closure of \(\mathcal{L}^T/\mathbb{F}_q(t)\) is \(\mathcal{L}/\mathbb{F}_q(t)\) itself. In our setting, this is the case even though it is not included in the definition.

In this section, we want to define the covers corresponding to \(G_N\)-extensions, namely strong \((N, G)\)-covers. These will be \((N, G)\)-covers satisfying certain maximality condition, which we define below.

Let the notation be as above. Let \(m = |N| = |G/T|\), and

\[
\rho : G \hookrightarrow Sym(G/T) \quad \text{defined by} \quad g \mapsto \rho(g) : hT \mapsto ghT
\]

be the representation given by the action of \(G\) on the left coset space \(G/T\) where the action is multiplication from the left. Note that \(\rho\) is injective if and only if \(T\) has no nontrivial subgroup that is normal in \(G\), which is the case by assumption. There is the obvious natural isomorphism between \(Sym(G/T)\) and \(Sym(N)\), and we will identify them below. Also, when it is convenient, we will sometimes order the elements of \(G/T\) and identify \(Sym(G/T)\) with \(S_m\) below. Notice that the image of \(N\) in \(Sym(N) = Sym(G/T)\) is transitive (since \(\rho\) restricts to the regular representation of \(N\)). Below, abusing the notation, we write \(N\) and \(G\) for their images in \(Sym(G/T)\).

We remark that we used the splitting condition \(G = N \rtimes T\) here to get a representation of \(G \hookrightarrow Sym(G/T)\) for which both \(N\) and \(G\) have transitive images. This is an assumption of [21, Theorem 4.1.4], which is used below in Theorem 3.1.

Let \(\mathbb{K}\) be a field. Roughly speaking, an \((N, G)\)-cover defined over \(\mathbb{K}\) is a \(M\)-Galois branched cover \(Z \rightarrow \mathbb{P}^1_{\mathbb{K}}\), where \(N \leq M \leq G\) and \(Z\) is a connected smooth curve defined over \(\mathbb{K}\), such that it factors as \(Z \rightarrow \mathbb{P}^1_{\mathbb{K}'} \rightarrow \mathbb{P}^1_{\mathbb{K}}\) for some finite separable extension \(\mathbb{K}'/\mathbb{K}\) where \(Z \rightarrow \mathbb{P}^1_{\mathbb{K}'}\) is a regular \(N\)-Galois cover. We call an \((N, G)\)-cover strong if \(M = G\).

Below, in Definition 2.2, we define \((N, G)\)-covers more precisely. The definition below can be related to the one above as follows: given a cover \(Z \rightarrow \mathbb{P}^1_{\mathbb{K}}\) as above, take \(Y = Z/(T \cap M)\) below. For the converse, take \(Z\) to be the Galois closure of \(Y\). Notice that here we again use the existence of the complement \(T\) of \(N\) in \(G\).

Let \(Y/\mathbb{K}\) be a geometrically connected smooth curve and let \(b\) be a geometric point of \(\mathbb{P}^1_{\mathbb{K}}\). Let \(B\) be a proper closed reduced subscheme of \(\mathbb{P}^1_{\mathbb{K}}\) defined over \(\mathbb{K}\) of degree \(k\), and let \(U = \mathbb{P}^1_{\mathbb{K}} - B\). Let \(f : Y \rightarrow \mathbb{P}^1_{\mathbb{K}}\) be a branched cover of degree \(m = |N|\) with branch locus \(B\). Suppose that the branched cover comes with bijection

\[
\sigma : G/T \rightarrow f^{-1}(b).
\]

Given another geometric point \(b_1\) on \(\mathbb{P}^1_{\mathbb{K}}\) and a bijection \(\sigma_1 : Sym(G/T) \rightarrow f^{-1}(b_1)\), one says that \((b_1, \sigma_1)\) is \(G\)-equivalent to \((b, \sigma)\) if there exists a path\(^2\) \(\gamma \in \Pi_1(U/\mathbb{K}, b, b_1)\) such that \(\sigma^{-1}_1 \gamma \sigma \in G\) where \(\tilde{\gamma} : f^{-1}(b) \rightarrow f^{-1}(b_1)\) is the lift of \(\gamma\). An \((N, G)\)-structure on the cover \((Y, f)\) is the \(G\)-equivalence class of a tuple \((b, \sigma)\) as above, which is denoted by \([b, \sigma]_G\).

\(^2\)For definitions of paths and fundamental groups, please see [19, Chapter V] or [3].
Let \( \bar{Y} = Y \times_{\mathbb{R}} \bar{\mathbb{R}} \). If \( \bar{f} : \bar{Y} \to \mathbb{P}^1_{\bar{\mathbb{R}}} \) is a connected Galois cover then the group \( \text{Aut}(\bar{Y}/\mathbb{P}^1_{\bar{\mathbb{R}}}) \) acts on the geometric fiber \( f^{-1}(b) \), and the tuple \((b, \sigma)\) induces a representation

\[
\text{Aut}(\bar{Y}/\mathbb{P}^1_{\bar{\mathbb{R}}}) \hookrightarrow \text{Sym}(G/T) \quad \text{defined by } \alpha \mapsto \sigma^{-1} \alpha \sigma.
\]

Now, suppose that

(i) \( \bar{f} : \bar{Y} \to \mathbb{P}^1_{\bar{\mathbb{R}}} \) is a connected Galois cover with \( \text{Aut}(\bar{Y}/\mathbb{P}^1_{\bar{\mathbb{R}}}) = N \subseteq \text{Sym}(G/T) \).

(ii) \( \bar{f} : Y \times_{\mathbb{R}} \bar{\mathbb{R}} \to \mathbb{P}^1_{\bar{\mathbb{R}}} \) is a connected Galois cover with \( \text{Aut}(\bar{Y}/\mathbb{P}^1_{\bar{\mathbb{R}}}) = N \subseteq \text{Sym}(G/T) \).

(iii) The Galois group \( \text{Gal}(\bar{\mathbb{R}}(Z)/\bar{\mathbb{R}}(t)) \) is contained in \( G \subseteq \text{Sym}(G/T) \) where \( Z \) is the Galois closure of \( Y \).

Furthermore, an \((N, G)\)-cover is called strong if \( \text{Gal}(\bar{\mathbb{R}}(Z)/\bar{\mathbb{R}}(t)) = G \).

As mentioned above, an \((N, G)\)-cover \( f : Y \to \mathbb{P}^1_{\bar{\mathbb{R}}} \) is not a Galois cover in general but it becomes Galois after a base change with a finite extension \( \mathbb{R}'/\mathbb{R} \). The quotient \( M/N \), where \( M = \text{Gal}(\bar{\mathbb{R}}(Z)/\bar{\mathbb{R}}(t)) \subseteq G \), is the degree of this extension. In particular, if \( N = G \), then \( f : Y \to \mathbb{P}^1_{\bar{\mathbb{R}}} \) is in fact a Galois cover. For more details, see [21, Section 3.4.2].

Note that, since \( \mathbb{P}^1 \) is path connected, each \((N, G)\)-structure \([b, \sigma]_G\) on \((Y, f)\) can be represented by a tuple \((b, \sigma)\) for some bijection \( \sigma : G/T \to f^{-1}(b) \). If \( \sigma \) is such a bijection, then one can see (perhaps, after reading next section) that \([b, \sigma]_G = [(b, \sigma)]_G\) if and only if \( \sigma = \sigma g \) for some \( g \in G \). Therefore, if we fix the geometric point \( b \), an \((N, G)\)-cover in fact corresponds to a “\( G \)-orbit” \([\{Y, f, b, \sigma g \mid g \in G\}]\).

Let \((Y, f, [b, \sigma]_G)\) be an \((N, G)\)-cover and let \( \rho' : \text{Gal}(\bar{\mathbb{R}}(Z)/\bar{\mathbb{R}}(t)) \to G \) be the corresponding map. Note that each \((N, G)\)-structure on the cover \((Y, f)\) is represented by \((b, \sigma \mu)\) for some \( \mu \in \text{Sym}(G/T) \). So, let \mu \in \text{Sym}(G/T). If the tuple \([b, \sigma \mu]_G\) is an \((N, G)\)-structure on the cover \((Y, f)\) then \mu^{-1} \text{Im}(\rho') \subseteq G. In particular, if \text{Im}(\rho') = G, then \mu \in N_{\text{Sym}(G/T)}(G) – the normalizer of \( G \) in \( \text{Sym}(G/T) \) – whenever \([b, \sigma \mu]_G\) is an \((N, G)\)-structure on \((Y, f)\).

2.3. Monodromy groups of \((N, G)\)-covers.

Let the notation be as above.

Suppose that an \((N, G)\)-cover \((Y, f, [b, \sigma]_G)\) defined over \( \mathbb{R} \) with branch locus \( B \) is given. Let \( U := \mathbb{P}^1 - B \) and let \( M = \rho'(\text{Gal}(\mathbb{R}(Z)/\mathbb{R}(t))) \subseteq G \).

Then, the \( M \)-Galois cover \( Z \to \mathbb{P}^1_{\bar{\mathbb{R}}} \) induces a representation of the arithmetic fundamental group over \( \mathbb{R} \):

\[
\tilde{\rho} : \Pi_1(U/\mathbb{R}, b) \to M \subseteq \text{Sym}(G/T),
\]

where \( N \subseteq M \subseteq G \). It is defined by

\[
\gamma \mapsto \sigma^{-1} \gamma \sigma
\]
where $\tilde{\gamma} : f^{-1}(b) \to f^{-1}(b)$ is the lift of $\gamma$.

Likewise, the $N$-Galois cover $Y \times_{\mathfrak{R}} \mathfrak{R} \to \mathbb{P}^1_{\mathfrak{R}}$ induces a representation of the geometric fundamental group

$$\phi : \Pi_1(U/\mathfrak{R}, b) \to N \subseteq \text{Sym}(G/T).$$

The map $\phi$ is just the restriction of $\tilde{\phi}$ to $\Pi_1(U/\mathfrak{R}, b)$ and so we have a commutative diagram of morphism of groups:

$$\begin{array}{cccc}
1 & \to & \Pi_1(U/\mathfrak{R}, b) & \to & \Pi_1(U/\mathfrak{R}, b) & \to & G_{\mathfrak{R}} & \to & 1 \\
\phi & \downarrow & \tilde{\phi} & \downarrow & \tilde{\phi} & \downarrow & \phi \\
1 & \to & N & \to & G & \to & G/N & \to & 1
\end{array}$$

The image $\text{Im}(\tilde{\phi}) = M \subseteq G$ is called the arithmetic monodromy group of the cover $(Y, f)$ over $\mathfrak{R}$, and the image $\text{Im}(\phi) = N$ is the called the geometric monodromy group of the cover.

Conversely, let a diagram as in (3) be given. Then, the map $\tilde{\phi}$ corresponds an $M$-Galois cover $\tilde{f} : Z \to \mathbb{P}^1_{\mathfrak{R}}$ where $M = \text{Im}(\tilde{\phi})$. This means that the cover $Z \to \mathbb{P}^1_{\mathfrak{R}}$ comes with an action of $M$ so that the action of $\gamma \in \Pi_1(U/\mathfrak{R}, b)$ on $f^{-1}(b)$ is equal to the one of $\tilde{\phi}(\gamma) \in M$.

For $Y = Z/(T \cap M)$, the induced cover $f : Y \to \mathbb{P}^1_{\mathfrak{R}}$ is a (geometrically connected) $N$-cover after a base change to $\mathbb{F}_q$. Define a bijection $\sigma : G/T \to f^{-1}(b)$ as follows.

First of all, each coset in $G/T$ can be represented by $\tilde{\phi}(\gamma)$ for some $\gamma \in \Pi_1(U/\mathfrak{R}, b)$. Fix an $x \in f^{-1}(b)$, and define

$$\sigma_x : G/T \to f^{-1}(b) \text{ by } \tilde{\phi}(\gamma)T \mapsto \tilde{\gamma}(x)$$

where $\tilde{\gamma} : f^{-1}(b) \to f^{-1}(b)$ is the lift of $\gamma$. Since $Y \to \mathbb{P}^1_{\mathfrak{R}}$ is fixed by $T$, $\sigma_x$ is well defined. As $Y \times \mathfrak{R} \to \mathbb{P}^1_{\mathfrak{R}}$ is an $N$-cover, $N$ acts sharply transitively on $f^{-1}(b)$, and $\sigma_x$ is a bijection. Therefore, $(Y, f, [b, \sigma_x]_G)$ is an $(N, G)$-cover defined over $\mathfrak{R}$.

Note that the map $\phi_x : \Pi_1(U/\mathfrak{R}, b) \to \text{Sym}(G/T)$ induced by $(Y, f, [b, \sigma_x]_G)$ is $\tilde{\phi}$ itself. Because, for $\gamma_0, \gamma \in \Pi_1(U/\mathfrak{R}, b)$, we have

$$\tilde{\phi}_x(\gamma_0)(\tilde{\phi}(\gamma)T) = \sigma_x^{-1}\gamma_0\sigma_x(\tilde{\phi}(\gamma)T) = \sigma_x^{-1}\gamma_0\tilde{\gamma}(x) = \sigma_x^{-1}\gamma_0\tilde{\phi}(\gamma_0)T = \tilde{\phi}(\gamma_0)(\tilde{\phi}(\gamma)T).$$

Hence, giving an $(N, G)$-cover defined over $\mathfrak{R}$ is equivalent to giving such a diagram. In other words, in terms of monodromy, an $(N, G)$-cover is a cover with geometric monodromy $N$ and arithmetic monodromy at most $G$.

A diagram as above (in other words, an $(N, G)$-cover defined over $\mathfrak{R}$) is determined by a map $\tilde{\phi} : \Pi_1(U/\mathfrak{R}, b) \to G$. Below, abusing the notation, we sometimes denote an $(N, G)$-cover by such a map (instead of a diagram).

Notice that if one begins with another representative $(Y, f, b, \sigma g)$ of the $(N, G)$-cover, then one gets the map

$$g^{-1}\tilde{\phi} g : \Pi_1(U/\mathfrak{R}, b) \to M.$$
2.4. Strong \((N,G)\)-covers over \(\mathbb{F}_q\). Now, we will see what it means geometrically for two strong \((N,G)\)-covers defined over \(\mathbb{F}_q\) to be isomorphic.

Let \((Y, f, b, \sigma)\) and \((Y_1, f_1, b, \sigma_1)\) be tuples representing strong \((N,G)\)-covers defined over \(\mathbb{F}_q\) in the sense of Definition 2.2, and let \(\tilde{\phi}, \tilde{\psi} : \Pi_1(U/\mathbb{F}_q, b) \rightarrow G\) be the corresponding maps.

First, suppose that these covers are isomorphic; that is, there exists \(g \in G\) such that
\[
\tilde{\phi}(\gamma) = g^{-1} \tilde{\psi}(\gamma) g \quad \text{for all } \gamma \in \Pi_1(U/\mathbb{F}_q, b).
\]
Let \(\gamma_0 \in \Pi_1(U/\mathbb{F}_q, b)\) with \(\tilde{\phi}(\gamma_0) = g\). Observe that the conjugation by \(\gamma_0\) takes the subgroup \(\tilde{\phi}^{-1}(T)\) to the subgroup \(\tilde{\psi}^{-1}(T)\).

On the other hand, \(\Pi_1(U/\mathbb{F}_q, b) \cong \text{Gal}(\mathbb{F}_q/\mathbb{F}_q(t))\) where \(\mathbb{F}_q(t)\) is the maximal separable algebraic extension of \(\mathbb{F}_q(t)\) that is unramified outside of \(B\). We fix such an isomorphism and identify these two groups for the discussion below.

We see that the subgroup \(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q(Y)) = \tilde{\phi}^{-1}(T)\) is conjugate to the subgroup \(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q(Y_1)) = \tilde{\psi}^{-1}(T)\) in \(\text{Gal}(\mathbb{F}_q/\mathbb{F}_q(q))\). Therefore, the extensions \(\mathbb{F}_q(Y)/\mathbb{F}_q(t)\) and \(\mathbb{F}_q(Y_1)/\mathbb{F}_q(t)\) are isomorphic. This implies that there exists an \(\mathbb{F}_q\)-morphism
\[
\psi : Y \rightarrow Y_1 \quad \text{with } f = f_1 \psi.
\]
Let \(\gamma \in \Pi_1(U/\mathbb{F}_q, b)\). Let \(\tilde{\gamma} : f^{-1}(b) \rightarrow f^{-1}(b)\) and \(\tilde{\gamma}_1 : f_1^{-1}(b) \rightarrow f_1^{-1}(b)\) be its lift. The fact that \(f = f_1 \psi\) implies that \(\tilde{\gamma}_1 = \psi \tilde{\gamma} \psi^{-1}\). A small calculation shows that, for \(h := \sigma^{-1} \psi^{-1} \sigma_1\),
\[
\tilde{\phi}(\gamma) = h^{-1} \tilde{\phi}(\gamma) h.
\]
Since \(\text{Im}(\tilde{\phi}) = G\) and the equality holds for all \(\gamma \in \Pi_1(U/\mathbb{F}_q, b)\), this implies that \(z := h g^{-1} \in \text{Cen}_{\text{Sym}(G/T)}(G)\). Notice that the \((N,G)\)-structure \([b, \sigma z]_G\) on \((Y, f)\) is not equal to \([b, \sigma]_G\) unless \(z \in G\), but the covers \((Y, f, [b, \sigma z]_G)\) and \((Y, f, [b, \sigma]_G)\) are isomorphic (even though they may be different). In any case,
\[
\sigma_1^{-1} \psi \sigma z \in G \text{ for some } z \in \text{Cen}_{\text{Sym}(G/T)}(G).
\]
Now, suppose that there exists \(\mathbb{F}_q\)-morphism \(\psi : Y \rightarrow Y_1\) with \(f = f_1 \psi\) and \(\sigma_1^{-1} \psi \sigma z \in G\) for some \(z \in \text{Cen}_{\text{Sym}(G/T)}(G)\). Then, one can see that for \(g = (\sigma_1^{-1} \psi \sigma z)^{-1} \in G\) we have
\[
\tilde{\phi}(\gamma) = g^{-1} \tilde{\psi}(\gamma) g
\]
for all \(\gamma \in \Pi_1(U/\mathbb{F}_q, b)\); that is, the strong \((N,G)\)-covers are isomorphic. Thus, we proved:

**Proposition 2.4.** Two strong \((N,G)\) -covers \((Y, f, [b, \sigma]_G)\) and \((Y_1, f_1, [b, \sigma_1]_G)\) defined over \(\mathbb{F}_q\) are isomorphic if and only if there exists an \(\mathbb{F}_q\)-morphism \(\psi : Y \rightarrow Y_1\) with \(f = f_1 \psi\) such that \(\sigma_1^{-1} \psi \sigma \in G \cdot \text{Cen}_{\text{Sym}(G/T)}(G)\).

Let \(Z, Z_1\) be the Galois closures of \(Y, Y_1\), respectively. As discussed above, \(\mathbb{F}_q(Z)/\mathbb{F}_q(t)\) and \(\mathbb{F}_q(Z_1)/\mathbb{F}_q(t)\) are \(G_N\)-extensions. If the covers \((Y, f, [b, \sigma]_G)\) and \((Y_1, f_1, [b, \sigma_1]_G)\) are isomorphic then, by Proposition 2.4, the extensions \(\mathbb{F}_q(Y)/\mathbb{F}_q(t)\) and \(\mathbb{F}_q(Y_1)/\mathbb{F}_q(t)\) are isomorphic, and so are their Galois closures \(\mathbb{F}_q(Z)/\mathbb{F}_q(t)\) and \(\mathbb{F}_q(Z_1)/\mathbb{F}_q(t)\).

Conversely, if \(\mathcal{L}/\mathbb{F}_q(t)\) is a \(G_N\)-extension then \(\mathcal{L} = \mathbb{F}_q(Z_2)\) for some (not necessarily geometrically connected) \(G\)-cover \(Z_2 \rightarrow \mathbb{P}^1_{\mathbb{F}_q} \rightarrow \mathbb{P}^1_{\mathbb{F}_q}\) such that \(Z_2 \rightarrow \mathbb{P}^1_{\mathbb{F}_q}\) is aa geometrically connected \(N\)-cover. This gives a diagram as in (3), which in turn induces a strong \((N,G)\)-cover defined over \(\mathbb{F}_q\) by the discussion above.

Suppose that the \(G_N\)-extensions \(\mathbb{F}_q(Z)/\mathbb{F}_q(t)\) and \(\mathbb{F}_q(Z_1)/\mathbb{F}_q(t)\) are isomorphic. Then, the extensions fixed by \(T\), namely \(\mathbb{F}_q(Y)/\mathbb{F}_q(t)\) and \(\mathbb{F}_q(Y_1)/\mathbb{F}_q(t)\), are isomorphic. This means that there exists an \(\mathbb{F}_q\)-morphism \(\psi : Y \rightarrow Y_1\) such that \(f = f_1 \psi\).
Let $\sigma' := \psi^{-1}\sigma_1 : G/T \to f^{-1}(b)$. Then, $[b, \sigma']_G$ is an $(N, G)$-structure on $(Y, f)$ and the $(N, G)$-cover $(Y, f, [b, \sigma']_G)$ is isomorphic to $(Y_1, f_1, [b, \sigma_1]_G)$ by Proposition 2.4. As mentioned above, there are finitely many $(N, G)$-structures on $(Y, f)$; each given by $[b, \sigma\mu]_G$ for some $\mu \in \text{Sym}(G/T)$. Therefore, we have:

**Proposition 2.5.** There is a surjective map

$$\{\text{Strong } (N, G)\text{-covers defined over } \mathbb{F}_q\}/ \cong \to \{G_N\text{-extensions of } \mathbb{F}_q(t)\}/ \cong$$

defined by

$$(Y, f, [b, \sigma]_G) \mapsto \mathbb{F}_q(Z)/\mathbb{F}_q(t)$$

whose fibers’ size is bounded by $m!$ where $m = |G/T|$.

Note that, by the discussion above, the number of isomorphism classes of strong $(N, G)$-covers corresponding to a $G_N$ extension is in fact equal to $|N_{\text{Sym}(G/T)}(G)/\text{Cent}_{\text{Sym}(G/T)}(G)|$. As we are interested only in the order of growth of $Z_{N,G}(\mathbb{F}_q(t), X)$, this reduces the problem of counting $G_N$-extensions to counting strong $(N, G)$-covers.

### 2.5. An alternative description of $(N, G)$-covers over $\overline{\mathbb{F}}_q$.

Note that if the map $\tilde{\phi} : \Pi_1(U/\mathbb{A}, b) \to G$ corresponds to a $(N, G)$-cover with branch locus $B$, then it does not factor through $\Pi_1((\mathbb{P}^1 - B_0)/\mathbb{A}, b) \to G$ for any subscheme $B_0 \subset B$.

Geometrically, an $(N, G)$-cover over $\overline{\mathbb{F}}_q$ is simply a disjoint union of (connected) $N$-covers with an $G$-Galois structure. Below, we will give a characterization in terms of discrete invariants which will be useful in the rest of the paper.

Suppose that an $(N, G)$-cover is given corresponding to the diagram (3) with $\mathbb{A} = \overline{\mathbb{F}}_q$; that is, just a surjective map $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b) \to N$. By definition, the isomorphism class of the $(N, G)$ cover corresponds to the $G$-orbit $\{g^{-1}\phi g \mid g \in G\}$ of the map $\phi$.

By the argument in section 2.1, the map $\phi$ is determined by $\phi(\gamma_1), \ldots, \phi(\gamma_k)$ where $\gamma_1, \ldots, \gamma_k$ are the generators of the profinite group $\Pi_1(U/\overline{\mathbb{F}}_q, b)'$ in (2) and $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b)' \to N$ is the map induced by $\phi$. Therefore, the isomorphism class of the $(N, G)$-cover over $\overline{\mathbb{F}}_q$ corresponds to the $G$-orbit of the $k$-tuple

$$[(\phi(\gamma_1), \ldots, \phi(\gamma_k))]_G := \{(\phi(\gamma_1), \ldots, \phi(\gamma_k))^g \mid g \in G\}$$

where the action of $G$ is component-wise conjugation, and vice versa. Hence, after fixing the generators $\gamma_1, \ldots, \gamma_k$, the isomorphism classes of $(N, G)$-covers of $\mathbb{P}^1$ over $\overline{\mathbb{F}}_q$ with branch locus $B$ are in one-to-one correspondence with $G$-orbits of the $k$-tuples $(h_1, \ldots, h_k) \in N^k$ satisfying that $N = \langle h_1, \ldots, h_k \rangle$ and that $h_1 \ldots h_k = 1$. We will discuss this correspondence in detail in section 3.2.

### 3. Connected components of Hurwitz schemes

In this section, first, we will state some basic facts about the coarse moduli schemes of $(N, G)$-covers and $N$-covers, namely Hurwitz schemes. Then, we will discuss the decomposition of Hurwitz schemes into their almost-geometrically-connected components.

The work in sections 3.1 and 3.2 is due to Fried [12] and Wewers [21]. We give a summary of it below for the sake of the discussion.
3.1. Hurwitz schemes of \((N, G)\)-covers and \(N\)-covers. We count strong \((N, G)\)-covers by counting rational points on corresponding moduli schemes. There is not a moduli scheme whose \(\mathbb{F}_q\)-rational points parameterizing strong \((N, G)\)-covers defined over \(\mathbb{F}_q\) as the arithmetic monodromy is not preserved under extension of constants. But, we have such a scheme for \((N, G)\)-covers:

**Theorem 3.1.** [21, Theorem 4.1.4] There exists a smooth scheme \(\mathcal{H} = \mathcal{H}_{N,G}\) over \(\mathbb{Z}\) which is a coarse moduli scheme for \((N, G)\)-covers of \(\mathbb{P}^1\). Moreover, the fibers of the natural map

\[
\Delta : \{(N, G)\text{-covers of } \mathbb{P}^1 \text{ defined over } \mathbb{F}_q\} / \cong \mathcal{H}(\mathbb{F}_q)
\]

has size at most \(|H|\).

**Proof.** Wewers carries out a detailed construction of \(\mathcal{H}\) in [21, Section 4]. Let \(P \in \mathcal{H}(\mathbb{F}_q)\). By section 4.1.3 of [21] and [7], the obstruction to \(P\) arising from a cover lies in the second cohomology group \(H^2(\mathbb{F}_q, H)\). Since \(\mathbb{F}_q\) has cohomological dimension one, there is no obstruction. And, \(\Delta^{-1}(P)\) is parameterized by \(H^1(\mathbb{F}_q, H)\) which has size at most \(|H|\), see [21, Lemma 3.4.2]. \(□\)

Note that a \((N, N)\)-cover \(Y \to \mathbb{P}^1_{\mathbb{F}_q}\) is a regular \(N\)-cover, and vice versa. Therefore, there is a natural isomorphism \(\mathcal{H}_{N,N} \cong \mathcal{H}_N\) of the moduli schemes (as schemes over \(\mathbb{F}_q\)), where \(\mathcal{H}_N/\mathbb{F}_q\) is the coarse moduli scheme of regular \(N\)-covers, see [21, Proposition 4.2.2]. We will use this isomorphism later to relate \(\mathbb{F}_q\)-rational points on \(\mathcal{H}\) to \(\mathbb{F}_q\)-rational points on \(\mathcal{H}_N\), see Proposition 4.2 below.

3.2. Nielsen classes and Nielsen tuples. In what follows, we describe geometrically connected components of Hurwitz schemes \(\mathcal{H}/\mathbb{F}_q\) and the discrete invariants –so called Nielsen tuples– which parametrize them. For the details of the discussion below see [21, Section 4.3].

Let \(U_k\) be the configuration space of \(k\) distinct points on \(\mathbb{P}^1_{\mathbb{Z}}\). Note that \(U_k = \mathbb{P}^k - \delta_k\) where \(\delta_k\) is the discriminant locus. Let \(\mathcal{H}_k\) be a moduli scheme of \((N, G)\)-covers with degree-\(k\) branch locus, which is defined over \(\mathbb{Z}\).

Let \(B = \{b_1, ..., b_k\} \subset \mathbb{P}^1_{\mathbb{Q}}\) be a set of \(k\) distinct points; i.e. \(B \in U_k(\mathbb{Q})\). The natural map

\[
\pi : \mathcal{H}_k \to U_k
\]

taking a cover to its branch locus is \(\acute{e}tale\) when restricted over \(\mathbb{Z}[1/|N|]\) [21, Theorem 4.1.4]. On the other hand, the geometric fundamental group \(\Pi_1(U_k/\mathbb{Q}, B)\) is the profinite completion of the braid group \(B_n\) on \(n\) strands [18, III, Theorem 2.2], where the braid group \(B_n\) can be written in standard representation with generators \(Q_1, ..., Q_{k-1}\) and relations:

1. \(Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}\) for \(i = 1, ..., k-2\)
2. \(Q_iQ_j = Q_jQ_i\) for \(i, j = 1, ..., k-1\) with \(|i - j| > 1\)
3. \(Q_1Q_2...Q_{k-1}Q_{k-1}...Q_2Q_1 = 1\).

Let \(Ni_k(N)\) be the set of \(k\)-tuples \(\vec{h} = (h_1, ..., h_k)\) generating \(N\) and satisfying \(h_1...h_k = 1\). Note that \(G\) acts on the set of such \(k\)-tuples by component-wise-conjugation; denote the orbit of \(\vec{h}\) in this action by \([\vec{h}]_G\). We call \(G\)-orbits of such \(k\)-tuples Nielsen classes and denote the set of Nielsen classes by \(Ni_k(N, G)\). We set \(Ni(N, G) := \bigsqcup_{k \geq 0} Ni_k(N, G)\).

Let \(U := \mathbb{P}^1_{\mathbb{Q}} - B\). Let \(\gamma_1, ..., \gamma_k\) be a generating set for the geometric fundamental group \(\Pi_1(U/\mathbb{Q}, b)\) as in section 2.1. Now, given a Nielsen class \([\vec{h}]_G \in Ni_k(N, G)\), one has surjective homomorphisms

\[
\phi : \Pi_1(U/\mathbb{Q}, b) \twoheadrightarrow N
\]
modulo conjugation with elements of $G$. Thus, such an orbit $[\bar{h}]_G \in Ni(N,G)$ and branch locus $B$ induces a $(N,G)$-cover of $\mathbb{P}^1$ defined over $\bar{Q}$, and vice versa. Hence, after fixing such a set of generators of $\Pi_1(U/\bar{Q},b)$, one gets a one-to-one correspondence between the set $Ni_k(N,G)$ of Nielsen classes and $(N,G)$-covers of $\mathbb{P}^1$ defined over $\bar{Q}$ with branch locus $B$.  

In summary, there is a bijection between $Ni_k(N,G)$ and the fiber $\pi_{\bar{Q}}^{-1}(B)$, where $\pi_{\bar{Q}} : \mathcal{H}_k \otimes_{\bar{Z}} \bar{Q} \to U_k \otimes_{\bar{Z}} \bar{Q}$. This bijection induces a well-known action of the braid group $B_n$ on $Ni_k(N,G)$ which is given by

$$Q_{\bar{1}}[(h_1, ..., h_k)]_N := [(h_1, ..., h_i h_{i+1} h_i^{-1}, h_i, ...h_k)]_N.$$ 

Thus, the connected components of $\mathcal{H} \otimes_{\bar{Z}} \bar{Q}$ correspond to the braid group orbits on $Ni(N,G)$.

It is known that the connected components of $\mathcal{H}_k \otimes_{\bar{Z}} \bar{Q}$ are in bijection with the connected components of $\mathcal{H}_k \otimes_{\bar{Z}} \bar{F}_q$, see [21, Corollary 4.2.3] and the paragraph coming right after its proof. Therefore, this induces a one-to-one correspondence between the connected components of $\mathcal{H} \otimes_{\bar{Z}} \bar{F}_q$ and the braid group orbits on $Ni(N,G)$.

Given a $k$-tuple $\bar{C} = (C_1, ..., C_k)$ of conjugacy classes of $N$, set

$$[\bar{C}]_G = \{\bar{C}^x = (C_1^x, ..., C_k^x) \mid x \in G\}$$

to be the $G$-orbit of the $k$-tuple of the conjugacy classes. One defines $Ni([\bar{C}]_G)$ to be the set of $[\bar{h}]_G \in Ni_k(N,G)$ such that, after some permutation of the entries of $h, h_i \in C_i$ for all $i$. Clearly, $Ni([\bar{C}]_G)$ is closed under the braid group action. Therefore, there is a closed subscheme (a priori defined over $\bar{F}_q$ and possibly empty) of $\mathcal{H} \otimes_{\bar{Z}} \bar{F}_q$ corresponding to $G$-orbit $[\bar{C}]_G$ of the tuple $\bar{C} = (C_1, ..., C_k)$, denoted by $\mathcal{H}_{[\bar{C}]_G}$, which parameterizes $(N,G)$-covers with ramification data $[\bar{C}]_G$. Thus, one has the decomposition over $\bar{F}_q$:

$$\mathcal{H} \otimes_{\bar{Z}} \bar{F}_q = \bigsqcup_{[\bar{C}]_G} \mathcal{H}_{[\bar{C}]_G}$$

where the union runs over the $G$-orbits of (unordered) tuples of conjugacy classes. By [21, section 4.3.1], a Galois transformation $\sigma \in G_{\bar{F}_q}$ acts on these components as follows:

$$H_{[\bar{C}]_G}^\sigma := H_{[\bar{C}^\sigma]_G}$$

where the action of $\sigma$ on the Nielsen tuple $\bar{C}$ is defined via cyclotomic character as mentioned in the introduction.

Likewise, taking $G$ to be $N$ in the discussion above, we get the one-to-one correspondence between the geometrically connected components of $\mathcal{H}_{N,N} \otimes_{\bar{Z}} \bar{F}_q$ and the braid group orbits on $Ni(N,N)$. Notice that, for an (unordered) tuple $\bar{C} = (C_1, ..., C_k)$ of conjugacy classes of $N$, $[\bar{C}]_G = \bar{C}$. And, the set $Ni([\bar{C}]_G) = Ni(\bar{C})$ is closed under the braid group action. Since $\mathcal{H}_N \cong \mathcal{H}_{N,N}$, one has the decomposition

$$\mathcal{H}_N \otimes_{\bar{Z}} \bar{F}_q = \bigsqcup_{\bar{C}} \mathcal{H}_{\bar{C}}.$$ 

One of the fundamental difficulties we encounter is that $\mathcal{H}_{\bar{C}}/\bar{F}_q$ is not necessarily connected; we will deal with this problem in Section 5. In summary, we have:

**Theorem 3.2.** [21, Chapter 4] For each $G$-orbit of $k$-tuples of conjugacy classes $[\bar{C}]_G = \{\bar{C}^x = (C_1, ..., C_k)^x \mid x \in G\}$ of $N$, there is a Hurwitz scheme $\mathcal{H}_{[\bar{C}]_G}$ (a priori defined over $\bar{F}_q$ and possibly empty) which is a coarse moduli scheme for $(N,G)$-covers $Y \to \mathbb{P}^1/\bar{F}_q$.

---

3The discussion in this paragraph is also valid over $\bar{F}_q$ by the argument in section 2.1 because $(q, |N|) = 1$. 
with ramification data \([\bar{C}]_G\). A Galois transformation \(\sigma \in G_{\bar{F}_q}\) acts on \(H_{[\bar{C}]}\) by \(H^\sigma_{[\bar{C}]} = H_{[\bar{C}^\sigma]}\) where the action of the Galois group on Nielsen tuple \(\bar{C}\) is defined via the cyclotomic character.

Moreover, the map \(\pi : H_{[\bar{C}]} \to U_k \otimes_{\mathbb{Z}} \bar{F}_q\) sending a cover to its branch locus is étale and geometric points of the fiber over \(B \in U_k(\bar{F}_q)\) can be identified with \(\text{Ni}([\bar{C}]_G)\). The action of the braid group \(B_n\) on \(\text{Ni}([\bar{C}]_G)\) is given by

\[Q_i[(h_1, ..., h_k)]_G = [(h_1, ..., h_i h_{i+1} h_i^{-1}, h_i, ..., h_k)]_G\]

and, geometrically connected components of \(H_{[\bar{C}]}\) correspond to the Braid group orbits on \(\text{Ni}([\bar{C}]_G)\).

4. The components parameterizing strong \((N, G)\)-covers

In this section, we will determine the components that parameterize the covers we want to count.

The purpose of this section is to prove Proposition 4.2 below. Note that the arithmetic monodromy group of a \((N, G)\)-cover is a subgroup of \(G\) containing \(N\) and we want to count the ones defined over \(\bar{F}_q\) whose arithmetic monodromy group is exactly \(G\), namely \(G_N\) covers defined over \(\bar{F}_q\).

Let \(H(\mathbb{F}_q)^G\) be the subset of \(H(\bar{F}_q)\) consisting of all the points parameterizing strong \((N, G)\)-covers defined over \(\mathbb{F}_q\); that is

\[H(\mathbb{F}_q)^G := \Delta(\{\text{strong } (N, G)\text{-covers of } \mathbb{F}_q \text{ defined over } \bar{F}_q\}/ \cong)\]

where \(\Delta\) is the natural map in Theorem 3.1. Below, we determine the components whose \(\mathbb{F}_q\)-rational points parameterize strong \((N, G)\)-covers defined over \(\mathbb{F}_q\).

Let \(G' \subseteq G\) containing \(N\) and let \(H' = H_{N,G'}\) be a coarse moduli scheme for \((N, G')\)-covers over \(\mathbb{Z}[1/|N|]\). Then, the natural map

\[\Lambda_G' : H' \to H\]

is an étale cover of degree \(|G/G'\text{Cen}_N(G')|\) and the map \(\pi' : H' \to U_k\) factors through \(\pi : H \to U_k\), see [12, Section 6.1] and [21, Section 4.2].

Taking \(G' = N\) above, using the canonical isomorphism \(H_N \cong H_{N,N}/\mathbb{F}_q\) and simplifying the notation, we obtain an étale cover

\[\Lambda : H_N \to H/\mathbb{F}_q\]

of degree \(|T'| = |G/NH|\) where \(H = \text{Cen}_N(N)\) and \([\bar{h}] := [\bar{h}]_N\).

Note that if \(H_{\bar{C}}\) is a component of \(H_N\) defined over \(\mathbb{F}_q\), then \(\Lambda\) restricts to a Galois cover

\[\Lambda : H_{\bar{C}} \to H_{[\bar{C}]}\]

with automorphism group \(T' = G/NH\). If \(P\) is a geometric point on \(H/\mathbb{F}_q\) corresponding to a Nielsen class \([\bar{h}]_G := [(h_1, ..., h_k)]_G\), then a point \(Q \in \Lambda^{-1}(P)\) corresponds the Nielsen class \([\bar{h}^x]\) for some \(x \in G\) where \(x\) acts on the \(k\)-tuple \((h_1, ..., h_k)\) by component-wise conjugation. Since the action of \(NH\) on \([\bar{h}]\) is trivial and \(h_1, ..., h_k\) generate \(N\), there exists a unique \(x \in T'\) such that \(Q\) parameterizes the \(N\)-cover corresponding to the Nielsen class \([\bar{h}^x]\).

Let \(H^1(\mathbb{F}_q, T')\) be the first Galois cohomology group where the action of \(G_{\bar{F}_q}\) is taken to be trivial on \(T'\). Note that \(H^1(\mathbb{F}_q, T') = \text{Hom}(G_{\bar{F}_q}, T') \cong T'\). For \(\zeta \in H^1(\mathbb{F}_q, T')\), let \(H_N^\zeta\) denote the \(\zeta\)-twist of \(H_N\) via the composition of \(\zeta\) with the embedding of \(T'\) in \(\text{Aut}(H_N/H)\).
Lemma 4.1. With the notation above, we have:

$$\Lambda^{-1}(\mathcal{H}(\mathbb{F}_q)) = \bigsqcup_{\zeta \in H^1(\mathbb{F}_q, T')} \mathcal{H}_N^\zeta(\mathbb{F}_q).$$

Proof. Let $P \in \mathcal{H}(\mathbb{F}_q)$. Then, $P$ parameterizes a $(N, G)$-cover defined over $\mathbb{F}_q$ corresponding to a commutative diagram:

$$
\begin{array}{cccccc}
1 & \longrightarrow & \Pi_1(U/\mathbb{F}_q, b) & \longrightarrow & \Pi_1(U/\mathbb{F}_q, b) & \longrightarrow & G_{\mathbb{F}_q} & \longrightarrow & 1 \\
\phi & & \phi & & \phi & & \phi & & \phi & & 1 \\
1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & 1 \\
\end{array}
$$

Note that $P$ parameterizes the $(N, G)$-cover corresponding to Nielsen class $[(\phi(\gamma_1), \ldots, \phi(\gamma_k))]_N$, and the points of $\Lambda^{-1}(P)$ parameterize the $N$-covers corresponding to Nielsen classes $[(\phi(\gamma_1), \ldots, \phi(\gamma_k))]_N$ for $x \in T' = G/NH$.

Let $Q \in \Lambda^{-1}(P)$. Let $\zeta \in \text{Hom}(G_{\mathbb{F}_q}, T') = H^1(\mathbb{F}_q, T')$ be the composition of $\tilde{\phi}$ with the projection $G/N \to T'$. Since $H = \text{Cen}_G(N)$ acts trivially on $(N, G)$-covers, for all $\sigma \in G_{\mathbb{F}_q}$, we have

$$Q^\sigma = Q^{\tilde{\phi}(\sigma)} = Q^\zeta(\sigma).$$

Therefore, $Q \in H_N^\zeta(\mathbb{F}_q)$, and $\Lambda^{-1}(P) \subseteq H_N^\zeta(\mathbb{F}_q)$.

Now, let $Q \in H_N^\zeta(\mathbb{F}_q)$ for some $\zeta \in H^1(\mathbb{F}_q, T')$. Say, $Q$ parameterizes the $N$-cover corresponding to the Nielsen class $[\bar{h}]$. Then, for $\sigma \in G_{\mathbb{F}_q}$, $Q^\sigma$ parameterizes the $N$-cover corresponding to the Nielsen class $[\bar{h}^\zeta(\sigma)]$. Therefore, the Nielsen class $[\bar{h}]_G$ is stable under the action of $G_{\mathbb{F}_q}$, because for all $\sigma \in G_{\mathbb{F}_q}$ we have

$$[\bar{h}]_G = \bigcup_{x \in T'} [\bar{h}^x]_N = \bigcup_{y \in T'} [\bar{h}^\zeta(\sigma)y]_N = [\bar{h}^\zeta(\sigma)]_G.$$

This implies that the point $P := \Lambda(Q)$, which parameterizes the $(N, G)$-cover corresponding to $[\bar{h}]_G$, is fixed by $G_{\mathbb{F}_q}$. That is, $P \in \mathcal{H}(\mathbb{F}_q)$, and thus $H_N^\zeta(\mathbb{F}_q) \subseteq \Lambda^{-1}(\mathcal{H}(\mathbb{F}_q))$. \hfill $\square$

Now, we want to determine the cocycles $\zeta \in H^1(\mathbb{F}_q, T')$ for which we have:

$$H_N^\zeta(\mathbb{F}_q) \subseteq \Lambda^{-1}(\mathcal{H}(\mathbb{F}_q)_G).$$

So, let $|T'| = d'$ and let $e$ be a positive integer with $1 \leq e \leq d'$. We denote the 1-cocycle sending Frob$_q$ to $\tau^e_1$ by $\zeta_e \in H^1(\mathbb{F}_q, T')$ where $\tau_1$ is the image of the generator $\tau \in T$ under the projection $T \to T'$. The following proposition tells us the schemes we should consider.

Proposition 4.2. We have the following decomposition

$$\Lambda^{-1}(\mathcal{H}(\mathbb{F}_q)_G) = \bigsqcup_{\substack{1 \leq e \leq d' \\ (e, d') = 1}} \mathcal{H}_N^\zeta_e(\mathbb{F}_q).$$

Proof. A $(N, G)$-cover defined over $\mathbb{F}_q$ with branch locus $B$ is a diagram of fundamental groups, for $U = \mathbb{P}^1 - B$: 
The cover corresponding to the above diagram is actually a strong \((N,G)\)-cover if and only if \(\tilde{\phi}\) is surjective \textit{i.e.} \(\tilde{\phi}(\text{Frob}_q) = \tau^r\) for some positive integer \(r\) with \(1 \leq r \leq d\) and \((r,d) = 1\).

Fix a set of generators \(\gamma_1,\ldots,\gamma_k\) of the profinite group \(\Pi_1(U/F_q, b)'\) as in (2). We abuse the notation and we let \(\phi : \Pi_1(U/F_q, b) \rightarrow N\) be the map induced by \(\phi\).

First, we want to prove the inequality \(\subseteq\). Let \(P \in \mathcal{H}(F_q)^G\) be a point corresponding to a strong \((N,G)\)-cover given by a diagram as above. Let \(Q \in \Lambda^{-1}(P)\).

Note that \(Q\) corresponds to the Nielsen class \([\langle \phi(\gamma_1), \ldots, \phi(\gamma_k) \rangle^x]\) for some \(x \in G\). Also, the action of \(\text{Frob}_q \in G_{\bar{F}_q}\) on \(\Lambda^{-1}(P)\) is the same as the action of \(\tilde{\phi}(\text{Frob}_q) \in G/N\) on \(\Lambda^{-1}(P)\).

This in turn is equivalent to the action of the class of \(\tilde{\phi}(\text{Frob}_q)\) in \(G/NH\) because \(H\) acts on \(\Lambda^{-1}(P)\) trivially. Since \(\tilde{\phi}\) is surjective, \(\tilde{\phi}(\text{Frob}_q)\) is a generator of \(G/N\) and the coset of \(\tilde{\phi}\) in \(T' = G/GH\) is a generator of \(T'\). This implies that \(\tilde{\phi}(\text{Frob}_q) = \tau^e_i\) for some \(e\) prime to \(d' = |T'|\). In summary, we have

\[
Q^{\text{Frob}_q} = Q^{\tilde{\phi}(\text{Frob}_q)} = Q^{\tau^e_i}
\]

for some unique integer \(e\) with

\[
1 \leq e \leq d' \quad \text{and} \quad (e,d') = 1.
\]

Therefore, \(Q \in \mathcal{H}_{\mathcal{C}_G}(F_q)\) and \(\Lambda^{-1}(\mathcal{H}(F_q)^G) \subseteq \bigsqcup_{(e,d)=1} \mathcal{H}_{\mathcal{C}_G}(F_q).

In what follows, we prove the inequality \(\supseteq\). Let \(e\) be a positive integer with \((e,d') = 1\) and \(1 \leq e \leq d'\) and let \(Q \in \mathcal{H}_{\mathcal{C}_G}(F_q)\). We want to show that \(\Lambda(Q) \in \mathcal{H}(F_q)^G\). In other words, we want to show that there exists a strong \((N,G)\)-cover

\[
\tilde{\phi} : \Pi_1(U/F_q, b) \twoheadrightarrow G
\]

such that \(\Delta(\tilde{\phi}) = \Lambda(Q)\) where

\[
\Delta : \{(N,G)\text{-covers of } \mathbb{P}^1/F_q\}/ \cong \mathcal{H}(F_q)
\]

is the natural map defined in Theorem 3.1.

Let \(P = \Lambda(Q)\). By Lemma 4.1, \(P \in \mathcal{H}(F_q)\). Let \(\tilde{\phi}_0 \in \Delta^{-1}(P)\) be a \((N,G)\)-cover defined over \(\bar{F}_q\); that is,

\[
\tilde{\phi}_0 : \Pi_1(U/F_q, b) \twoheadrightarrow G.
\]

Let \(G' := \text{Im}(\tilde{\phi}_0)\). We will construct a strong \((N,G)\)-cover \(\phi \in \Delta^{-1}(P)\) from the cover \(\tilde{\phi}_0\). Set \(H' = \text{Cen}_G(N)\).

\textbf{Step 1.} The group \(G'\) is not arbitrary. More precisely, the inclusion \(G' \hookrightarrow G\) induces the following commutative diagram:

\[
\begin{array}{cccccc}
1 & \longrightarrow & N/\text{Cen}(N) & \longrightarrow & G'/H' & \longrightarrow & G'/NH' & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & N/\text{Cen}(N) & \longrightarrow & G/H & \longrightarrow & G/NH & \longrightarrow & 1
\end{array}
\]
where vertical maps are isomorphisms.

**Proof.** The map $\bar{\phi}_0$ fits into the following commutative diagram:

\[
\begin{array}{cccccc}
1 & \rightarrow & \Pi_1(U/\mathbb{F}_q, b) & \rightarrow & \Pi_1(U/\mathbb{F}_q, b) & \rightarrow & G_{\mathbb{F}_q} & \rightarrow & 1 \\
\downarrow{[\phi_0]} & & \downarrow{[\bar{\phi}_0]} & & \downarrow{[\bar{\phi}_0]} & & \downarrow{[\bar{\phi}_0]} & \\
1 & \rightarrow & N/\text{Cen}(N) & \rightarrow & G/H & \rightarrow & G/NH & \rightarrow & 1
\end{array}
\]

Then, $\bar{\phi}_0(\text{Frob}_q) = \tau^f$ for some $f$ with $1 \leq f \leq d$. Note that $\tau^f$ is a generator of $G'/N$. Because $Q \in \Lambda^{-1}(P)$, the $N$-cover parameterized by $Q$ is given by the Nielsen class $[(\phi_0(\gamma_1), \ldots, \phi_0(\gamma_k)]$ for some $x \in G'$. As in equality (4), we have the following identity

\[Q^{\text{Frob}_q} = Q^{\phi_0(\text{Frob}_q)} = Q^{\tau^f}.
\]

On the other hand, $Q^{\text{Frob}_q} = Q^{e^e}$ since $Q \in \mathcal{H}^e_G(\mathbb{F}_q)$. Therefore, $Q^{e^e-f} = Q$ and $\tau^{e-f} \in NH$ (as the action of $G/NH$ on $\Lambda^{-1}(P)$ is sharply transitive). Equivalently, $\tau^e = \tau^f$ in $G/NH$. Since $(e, d') = 1$, $\tau^e$ generates $G/NH$ and so does $\tau^f$. Thus, $\tau^f$ is a generator for both $G'/G'H'$ and $G/NH$. This implies that the natural map

\[G'/N'H' \rightarrow G/NH
\]

induced by the inclusion $G' \rightarrow G$ is surjective. This map is in fact an isomorphism because its kernel is $G' \cap NH = N'H'$. This completes the proof of the first step.

Using the projection $G' \rightarrow G'H'$, we combine the diagrams (6) and (5) and get the following commutative diagram:

\[
\begin{array}{cccccc}
1 & \rightarrow & \Pi_1(U/\mathbb{F}_q, b) & \rightarrow & \Pi_1(U/\mathbb{F}_q, b) & \rightarrow & G_{\mathbb{F}_q} & \rightarrow & 1 \\
\downarrow{[\phi_0]} & & \downarrow{[\bar{\phi}_0]} & & \downarrow{[\bar{\phi}_0]} & & \downarrow{[\bar{\phi}_0]} & \\
1 & \rightarrow & N/\text{Cen}(N) & \rightarrow & G/H & \rightarrow & G/NH & \rightarrow & 1
\end{array}
\]

Now, we want to construct surjective maps

\[\phi : \Pi_1(U/\mathbb{F}_q) \rightarrow N \quad \text{and} \quad \bar{\phi} : G_{\mathbb{F}_q} \rightarrow G/N
\]

such that:

**Step 2.** We have the following commutative diagram of groups:

\[
\begin{array}{cccccc}
1 & \rightarrow & \Pi_1(U/\mathbb{F}_q, b) & \rightarrow & \Pi_1(U/\mathbb{F}_q, b) & \rightarrow & G_{\mathbb{F}_q} & \rightarrow & 1 \\
\downarrow{[\phi_0]} & & \downarrow{[\bar{\phi}_0]} & & \downarrow{[\bar{\phi}_0]} & & \downarrow{[\bar{\phi}_0]} & \\
1 & \rightarrow & N/\text{Cen}(N) & \phi & G/H & \rightarrow & G/NH & \bar{\phi} & 1 \\
\downarrow{1} & & \downarrow{\phi} & & \downarrow{\bar{\phi}} & & \downarrow{1} & \\
1 & \rightarrow & N & \rightarrow & G & \rightarrow & G/N & \rightarrow & 1
\end{array}
\]

**Proof.** We define $\phi$ to be the map $\phi_0 : \Pi_1(U/\mathbb{F}_q, b) \rightarrow N$ in diagram 6, and this commutes with the map $[\phi_0]$ by definition of $[\phi_0]$. So, we just need to define the map $\bar{\phi}$ in the diagram.

\[\text{Here, } \phi_0 : \Pi_1(U/\mathbb{F}_q)' \rightarrow N \text{ is the map induced by } \phi_0 \text{ as noted in section 2.1.}\]
Recall that \(|G/NH| = d', |NH/N| = d'' \) and \(|G/N| = d\) (so, we have \(d = d'd''\)). One can easily see that \((e + ad'd',d) = 1\) for some \(a\) with \(0 \leq a \leq d'' - 1\). So, let \(e' = e + ad' < d\) be such that \((e',d) = 1\).

Note that \(\tau^e = \tau^f = \tau^{e'}\) in \(G/NH\). Now, define
\[
\tilde{\phi} : G_{F_q} \to G/N \quad \text{as} \quad \text{Frob}_q \mapsto \tau^{e'}.
\]
The map \(\tilde{\phi}\) is surjective because \((e',d) = 1\). It also fits into the commutative diagram since \([\tilde{\phi}_0](\text{Frob}_q) = \tau^f = \tau^{e'} = \tilde{\phi}(\text{Frob}_q)\) in \(G/NH\). This completes the proof of the second step.

**Step 3.** There exists a surjective morphism \(\phi : \Pi_1(U/F_q, b) \to G\) such that we have the following commutative diagram:

\[
\begin{array}{ccccccccc}
1 & \longrightarrow & \Pi_1(U/F_q, b) & \longrightarrow & \Pi_1(U/F_q, b) & \longrightarrow & G_{F_q} & \longrightarrow & 1 \\
\downarrow{[\phi_0]} & & \downarrow{[\tilde{\phi}_0]} & & \downarrow{[\tilde{\phi}_0]} & & \downarrow{[\tilde{\phi}_0]} & & \downarrow{[\tilde{\phi}_0]} \\
1 & \longrightarrow & N/Cen(N) & \to & G/H & \to & \tilde{\phi} & \to & G/NH & \to & 1 \\
\end{array}
\]

\[
\begin{array}{ccccccccc}
1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & 1 \\
\end{array}
\]

**Proof.** The obstruction to the existence of \(\tilde{\phi}\) lies in \(H^2(F_q, H)\) [7, Theorem 4.3]. Since \(F_q\) has cohomological dimension 1, there exists such a lift. Since \(\phi\) and \(\tilde{\phi}\) are surjective, \(\phi\) is surjective; hence, the proof of the third step.

Now, as the final step, we claim that \(\tilde{\phi} : \Pi_1(U/F_q, b) \to G\) is the strong \((N,G)-\)cover we were looking for; that is, \(\tilde{\phi} \in \Delta^{-1}(P)\). It suffices to show that the \((N,G)-\)covers \(\phi_0\) and \(\tilde{\phi}\) are isomorphic over \(F_q\). This is obvious, because \(\phi_0 = \phi\) and so they both correspond to the Nielsen class \([[\phi(\gamma_1), ..., \phi(\gamma_k)]]_G\). We are done.

A **Nielsen tuple** is a tuple \(C\) of conjugacy classes of \(N\) or its \(G\)-orbit \([C]_G\). Given two Nielsen tuples \(C\) and \(C'\), we write \(C = C'\) if they differ only by a permutation of the entries, and we write \([C]_G = [C']_G\) if \(C' = C^x\) for some \(x \in G\). We denote their concatenation by \(\bar{C} + \bar{C}'\).

**Definition 4.3.** Given an integer \(1 \leq e \leq d'\) with \((e,d') = 1\) and Nielsen tuple \(\bar{C}\), we say \(\bar{C}\) is \(F_q\)-rational of type \(e\) if \(\bar{C}^q^{r_{e}} = \bar{C}\).

Recall that we want to count points in \(\mathcal{H}(F_q)^G\). Using Proposition 4.2 and Proposition 4.5 below, we will count points in \(\mathcal{H}_C^e(F_q)\) for each \(e\) and for all \(F_q\)-rational Nielsen tuples \(C\) of type \(e\), and then we will add them over all \(e\)'s with \(1 \leq e \leq d'\).

Note that the **type** of a Nielsen tuple \(\bar{C}\) is not necessarily unique. But, this does not create any double counting issues because we have:

**Lemma 4.4.** Let \(e, f\) be two different integers with \(1 \leq e < f \leq d'\). Then,
\[
\mathcal{H}_N^e(F_q) \cap \mathcal{H}_N^f(F_q) = \emptyset.
\]

**Proof.** Assume, to reach a contradiction, that there exists a point in the intersection. Then, this point parameterizes an \(N\)-cover defined over \(F_q\) corresponding to the Nielsen class \([\bar{h}]\). This means that \([\bar{h}^e] = [\bar{h}]\text{Frob}_q = [\bar{h}]^{r_f}\). So, \([\bar{h}]^{r_f^e} = [\bar{h}]\), and \(\bar{h}^{r_f^e} = \bar{h}^g\) for some \(g \in N\). Since the coordinates of \(\bar{h}\) generate \(N\), we have \(\tau^f g^{-1} \in \text{Cen}_G(N)\); that is, \(\tau^f g^{-1} = 1\) in \(T'\). Since \(1 \leq e < f \leq d'\) and \(T'\) is a cyclic group with generator \(\tau\) of order \(d'\), we get \(e = f\). A contradiction.

\(\square\)
The following proposition is our reason for defining $\mathbb{F}_q$-rational of type $e$ Nielsen tuples as in Definition 4.3.

**Proposition 4.5.** For every $e$ with $1 \leq e \leq d'$ and $(e,d') = 1$, we have

$$\mathcal{H}_N^\mathcal{C}(\mathbb{F}_q) = \bigcup_{\mathcal{C}^q r^e = \mathcal{C}} \mathcal{H}_N^\mathcal{C}(\mathbb{F}_q)$$

where the union runs over $\mathbb{F}_q$-rational Nielsen tuples $\mathcal{C}$ of type $e$.

**Proof.** Let $\bar{C} = (C_1, \ldots, C_k)$ be a Nielsen tuple. By taking $G = N$ in Theorem 3.2, we know that $G_{\mathbb{F}_q}$ acts on Nielsen tuple $\bar{C}$ via cyclotomic character. This means that $\bar{C}^\text{Frob} = \bar{C}^q$ (here $\bar{C}^q = (C_1^q, \ldots, C_k^q)$ and $C_i^q$ denotes the conjugacy class of the $q$th power of a representative of the conjugacy class $C_i$). Therefore, by Theorem 3.2, the corresponding component $\mathcal{H}_N^\mathcal{C}$ is defined over $\mathbb{F}_q$ if and only if $\bar{C}^q r^e = \bar{C}$. Applying decomposition in section 3.2, we get the desired decomposition. \hfill \square

5. **Proof of Theorem 1.2**

Let $f : Y \to \mathbb{P}^1_{\mathbb{F}_q}$ be a strong $(N,G)$-cover. Then, its Galois closure $\tilde{f} : Z \to \mathbb{P}^1_{\mathbb{F}_q}$ is a connected $G$-Galois cover defined over $\mathbb{F}_q$. As in section 1.1, we consider degree-$n$ cover $C \to \mathbb{P}^1_{\mathbb{F}_q}$ where $C = Z/S$ and $S \subseteq G$ is the stabilizer of $1 \in \{1, \ldots, n\}$.

**Definition 5.1.** The discriminant of a strong $(N,G)$-cover $(Y,f)$ is the integer $q^{r(Y,f)}$ where $r(Y,f)$ is the degree of the ramification divisor\(^5\) of the degree-$n$ cover $C \to \mathbb{P}^1_{\mathbb{F}_q}$.

Instead of counting $G_N$-extensions, we will count corresponding strong $(N,G)$-covers. Here is the definition of the counting function of covers:

**Definition 5.2.** Given a number $X$, $\mathcal{Z}_{N,G}(\mathbb{F}_q, X)$ is the number of isomorphism classes of strong $(N,G)$-covers $(Y,f)$ defined over $\mathbb{F}_q$ with $q^{r(Y,f)} < X$.

Note that the definition of the discriminant of a cover above and the one of extensions in section 1.1 are the same by definition; that is, $r(\mathcal{L}/\mathbb{F}_q(t)) = r(Y,f)$ where $\mathcal{L} = \mathcal{F}_q(Z)$. Therefore, the counting function $\mathcal{Z}_{N,G}(\mathbb{F}_q, X)$ of covers coincide with the one $\mathcal{Z}_{N,G}(\mathbb{F}_q(t), X)$ of extensions since strong $(N,G)$-covers correspond to $G_N$-extensions.

Recall that Hurwitz schemes $\mathcal{H}/\mathbb{F}_q$ of $(N,G)$-covers are not fine moduli schemes unless $H = 1$. However, since the fiber of the map $\Delta$ in Theorem 3.1 is bounded by the order $|G|$ of the group, asymptotic of the counting function $\mathcal{Z}_{N,G}(\mathbb{F}_q, X)$ of covers is a constant multiple of the asymptotic of the corresponding counting function of rational points. Since we are only interested in the order of growth of $\mathcal{Z}_{N,G}(\mathbb{F}_q, X)$, Theorem 3.1 and Proposition 4.2 reduces the problem of counting covers to counting rational points on certain twists of Hurwitz schemes $\mathcal{H}_N/\mathbb{F}_q$.

By Heuristic 1.3 and Proposition 4.2, the problem of counting rational points on Hurwitz schemes $\mathcal{H}_N/\mathbb{F}_q$ boils down to determining the geometrically connected components of $\mathcal{H}_N/\mathbb{F}_q$. Note that this is a very old and difficult problem with a rich history, going all the way back to Hurwitz [13] and Clebsch [4].

In this section, we will mainly define two counting functions, the first one ($h_{cc}$ in Definition 5.3 below) is indexed by the connected components of Hurwitz schemes and the second ($h_{ns}$ in

---

\(^5\)See section 1.1 for the definition of ramification divisor.
Definition 5.3 below) is indexed by Nielsen tuples. Determining the asymptotics for the first counting function is a geometric problem, whereas the asymptotics for the second function is a combinatorial one. The main purpose of section 5 is to prove Proposition 5.4 which states that these two counting functions are actually asymptotic to each other.

5.1. Counting functions. For a given $k$-tuple $C = (C_1, ..., C_k)$ of conjugacy classes of $N$, set $|\bar{C}| := k$ to be the length of the tuple and $r(\bar{C}) := \sum_{i=1}^{k} \text{ind}(C_i)$ where $\text{ind}(C)$ is the index of a representative of the conjugacy class $C$. Let $\Sigma_{r,e}$ be the set of $\mathbb{F}_q$-rational Nielsen tuples $\bar{C}$ of type $e$ with $r(\bar{C}) = r$; and let $\Sigma_r$ be the set of Nielsen tuples $\bar{C}$ with $r(\bar{C}) = r$. Let $\Sigma_G^r$ be the set of Nielsen tuples $[\bar{C}]_G$ with $r(\bar{C}) = r$. Finally, let $\mathcal{H}_{[\bar{C}]_G}(\mathbb{F}_q)^G$ denote the subset of $\mathcal{H}_{[\bar{C}]_G}(\mathbb{F}_q)$ consisting of all the points in $\mathcal{H}_{[\bar{C}]_G}(\mathbb{F}_q)$ parameterizing strong $(N, G)$-covers.

**Definition 5.3.** We will need the following counting functions:

i. $h_C(q, r) := \sum_{[\bar{C}]_G \in \Sigma^q_G} |\mathcal{H}_{[\bar{C}]_G}(\mathbb{F}_q)^G|$.  
ii. $h_N(q, r, e) := \sum_{\bar{C} \in \Sigma_{r,e}} |\mathcal{H}_{\bar{C}}^e(\mathbb{F}_q)|$ and $h_N(q, r) := \sum_{(e, d') = 1}^{1 \leq e \leq d'} h_N(q, r, e)$.  
iii. $h_{cc}(q, r, e) := \sum_{\bar{C} \in \Sigma_{r,e}} q^{\bar{C}}$ where the sum runs over all geometrically connected components of $\mathcal{H}_{\bar{C}}^e$’s defined over $\mathbb{F}_q$ where $\bar{C} \in \Sigma_{r,e}$ and $h_{cc}(q, r) := \sum_{(e, d') = 1}^{1 \leq e \leq d'} h_{cc}(q, r, e)$.  
iv. $h_{ns}(q, r, e) := \sum_{\bar{C} \in \Sigma_{r,e}} q^{\bar{C}}$ and $h_{ns}(q, r) := \sum_{(e, d') = 1}^{1 \leq e \leq d'} h_{ns}(q, r, e)$.

Let us briefly explain what these counting functions actually keep track of: Roughly speaking, we want to “understand” the counting function $h_G$ as we want to count points in $\mathcal{H}_{[\bar{C}]_G}(\mathbb{F}_q)$ that parameterize certain strong $(N, G)$-covers. By Proposition 4.2, this is equivalent to counting points in $\mathcal{H}_{\bar{C}}^e(\mathbb{F}_q)$ which parametrizes certain $N$-covers and so we denote the corresponding counting function by $h_N$. Provided with Heuristic 1.3, we see that $h_N$ is the same as $h_{cc}$ which basically “counts” the geometrically connected components of $\mathcal{H}_N/\mathbb{F}_q$ (and its twists). As the combinatorial problem of counting geometrically connected components is very hard, we will relate $h_{cc}$ to an easy-to-understand combinatorial counting function $h_{ns}$ which essentially counts certain Nielsen tuples.

If $\mathcal{H}_{\bar{C}}^e$ were geometrically connected for all $\mathbb{F}_q$-rational Nielsen tuples $\bar{C}$ of type $e$ and for all relevant $e$, then the sum $\sum_{q' < X} h_{cc}(q, r)$ would be equal to $\sum_{q' < X} h_{ns}(q, r)$ and it would be enough to find the asymptotics for the combinatorial sum $\sum_{q' < X} h_{ns}(q, r)$. Unfortunately, in general, this is not the case.

In this section, we want to prove that the sums $\sum_{q' < X} h_{cc}(q, r)$ and $\sum_{q' < X} h_{ns}(q, r)$ are asymptotic to each other. In other words, we will see that there are “many” $\mathbb{F}_q$-rational Nielsen tuples $\bar{C}$ such that $\mathcal{H}_{\bar{C}}^e$ possesses a geometrically connected component defined over $\mathbb{F}_q$ for all $e$ and the number of these components is bounded by positive constant depending only on the group $G$. Thus, we will reduce the problem to computing the sum $\sum_{q' < X} h_{ns}(q, r)$. More precisely, the purpose of this section is to prove the following proposition, which is the adapted version of [10, Theorem 3.2] to our setting:

**Proposition 5.4.** Let $e$ be such that $1 \leq e \leq d'$ and $(e, d') = 1$. There exist positive constants $m, c_1$ depending on $G$ such that

$$\sum_{r < R - m} h_{ns}(q, r, e) < \sum_{r < R} h_{cc}(q, r, e) < c_1 \sum_{r < R} h_{ns}(q, r, e).$$
By the lemma below, we have the right-hand-side inequality.

**Lemma 5.5.** [10, Lemma 3.3] There exists a constant $c_1$ such that $n(\bar{C}) < c_1$ for all $\bar{C}$ where $n(\bar{C})$ is the number of braid group orbits on $Ni(\bar{C})$.

As for the inequality on the left-hand-side, we need a theorem of Conway-Parker and Fried-Völklein.

5.2. CPFV-Theorem and two technical lemmas. As for the inequality on the left-hand-side, we again adapt the strategy of Ellenberg-Venkatesh where they use (to prove the inequality) a result controlling the geometrically connected components of Hurwitz schemes. The first such result along the lines presented here is attributed to Conway and Parker– the first version of such a theorem to appear in print is due to Fried and Völklein [12].

**Lemma 5.6.** (Conway-Parker)[12, Appendix] Let $N'$ be a finite group such that the Schur multiplier $M(N')$ is generated by commutators. Then, there exists a constant $c$ such that for any Nielsen tuple $E$ of $N'$ which contains at least $c$ copies of each nontrivial conjugacy classes of $N'$ the corresponding Hurwitz space $H_E$ is geometrically connected.

We will need the next two technical lemmas to prove Proposition 5.4. First of them is needed to apply Lemma 5.6 to our setting.

**Lemma 5.7.** There exists a commutative diagram of finite groups

\[
\begin{array}{ccc}
\tilde{G} & \xrightarrow{\pi} & G \\
\downarrow & & \downarrow \\
\tilde{N} & \xrightarrow{\pi'} & N'
\end{array}
\]

such that the Schur multiplier $M(N')$ is generated by commutators, where the vertical maps are inclusions and horizontal maps are surjections.

**Proof.** By Lemma 1 of [12], there exists an extension of groups

\[
1 \longrightarrow M' \longrightarrow N' \longrightarrow N \longrightarrow 1
\]

such that Schur multiplier $M(N')$ of $N'$ is generated by commutators and Schur multiplier $M(N) \cong M'$. Let $M := \text{Ind}_G^N(M')$ be the induced $G$-module. Then, by Shapiro’s lemma, $H^2(N, M')$ is isomorphic to $H^2(G, M)$. Let

\[
1 \longrightarrow M \longrightarrow \tilde{G} \xrightarrow{\pi} G \longrightarrow 1
\]

be an extension which corresponds to the extension above via the isomorphism $H^2(N, M') \cong H^2(G, M)$, and let $\tilde{N} = \pi^{-1}(N)$. Now, the evaluation morphism $\tilde{M} \rightarrow M'$ defined by $f \mapsto f(1)$ induces the following surjective morphism of groups $\pi' : \tilde{N} \rightarrow N'$. One can check that these extensions fits into the desired commutative diagram above and complete the proof.\[\square\]

Let $\pi : \tilde{G} \rightarrow G$ be a surjective morphism of finite groups with $\tilde{N} := \pi^{-1}(N)$ as in Lemma 5.7. Clearly, $\tilde{N}$ is normal subgroup of $\tilde{G}$ of index $d$ with cyclic quotient. Let’s fix and denote $\tilde{\tau} \in \tilde{G}$ generating $\tilde{T} := \tilde{G}/\tilde{N}$ with $\pi(\tilde{\tau}) = \tau$. Let $\tilde{H} = \text{Cen}_{\tilde{G}}\tilde{N}$ and $\tilde{T}' := \tilde{G}/\tilde{N}\tilde{H}$. Simplifying the notation, $\tilde{\tau}$ will also denote its image in $\tilde{T}$ and $\tilde{\tau}$ will denote its image in $\tilde{T}'$. Note that the map $\tilde{\pi} : \tilde{T}' \rightarrow T'$ induced by $\pi$ is an isomorphism. Recall that $\tilde{G}$ acts on $\tilde{N}$-covers and...
this induces an action of $\tilde{T}'$ on $\mathcal{H}_\varphi$ as in Section 3. Namely, if a $\tilde{N}$-cover is induced by a morphism, for $U = \mathbb{P}^1 - B$, $\phi : \Pi_1(U/\overline{\mathbb{F}}_q, b) \to \tilde{N}$ then the action of $x \in G$ is defined by
\[ \phi^x(\gamma) := x^{-1}\phi(\gamma)x \quad \text{for all } \gamma \in \Pi_1(U/\overline{\mathbb{F}}_q, b). \]
One defines the cocycles $\tilde{\zeta}_e \in H^1(\mathbb{F}_q, \tilde{T}')$ by $\text{Frob}_b \mapsto \tilde{\tau}_b^e$ for all $e$ with $1 \leq e \leq d'$.

The arguments in the proof of the following Lemma and Proposition 5.4 are due to Ellenberg and Venkatesh, see [10, Section 3]. We present a modified version of their proof here for the sake of completeness. Here is the second lemma we need to prove Proposition 5.4:

**Lemma 5.8.** For every $e$ with $1 \leq e \leq d'$ and $(e, d') = 1$ there exists a finite set of $\mathbb{F}_q$-rational Nielsen tuples $\bar{D}_1, \ldots, \bar{D}_r$ of type $e$ in $\tilde{N}$ such that for any given $\mathbb{F}_q$-rational Nielsen tuple $\bar{D}$ of type $e$, $\mathcal{H}_{\bar{D}_1 + \cdots + \bar{D}_r}(\overline{\mathbb{F}}_q)$ is nonempty for some $i$.

**Proof.** We first claim that $(q, |\tilde{N}|) = 1$. By our assumption, $(q, |G|) = 1$, and so $(q, |\tilde{N}|) = 1$. Since the exponent of the Schur multiplier $M(N)$ of $N$ divides the order of the group $N$ and since $M' \cong M(N)$, we have $(q, |M'|) = 1$. Therefore, the order of $M := \text{Ind}_G^N(M')$ is coprime to $q$. Hence, $(q, |\tilde{N}|) = 1$ and $(q, |\tilde{N}|) = 1$ as $\tilde{N} \subseteq G$.

Now, we can replace $\tilde{r}$ with $\tilde{r}^e$ in the proof below so we may assume that $e = 1$. Let $A \leq \tilde{N}$ be the subgroup generated by the products $\prod h_i$ where $(h_1, \ldots, h_l)$ represents a Nielsen tuple $\bar{D}$ of type $e = 1$; i.e. $\bar{D}^q = \bar{D}^\tilde{r}$. We will show that for all $x \in A$, there exists a $k$-tuple $\bar{h} = (h_1, \ldots, h_k) \in \tilde{N}^k$ such that
\[ -h_1 \cdots h_k = x \]
\[ -\tilde{N} = (h_1, \ldots, h_k) > \bar{h} \]
represents a $\mathbb{F}_q$-rational Nielsen tuple $\bar{D}$ in $\tilde{N}$ with $\bar{D}^q = \bar{D}^\tilde{r}$.

It suffices to show for $x = 1$, because: If $\bar{h} = (h_1, \ldots, h_k)$ is such a tuple with $h_1 \cdots h_k = 1$ and if $\tilde{x} = (x_1, \ldots, x_k)$ is a $k$-tuple having product $x$ and representing a Nielsen tuple $\bar{D}'$ with $\bar{D}'^q = \bar{D}'^\tilde{r}$, then we can just concatenate $\tilde{g}$ with $\tilde{x}$ and thus, get such a tuple having multiple $x$.

So, let $\tilde{g} = (g_1, \ldots, g_s)$ be a generating set for $\tilde{N}$ which represents a Nielsen tuple $\bar{D}_0$. Since $(q, |\tilde{N}|) = 1$, there exists an integer $m$ such that $q^m \equiv 1 \pmod{|\tilde{N}|}$. Then, for $\bar{D}_1 = \prod_{i=0}^{m-1} \bar{D}_0^i$, we have the equality $\bar{D}_1^q = \bar{D}_1$. Set $\bar{D} = \sum_{i=0}^{k-1} \bar{D}_i^q$. Obviously, $\bar{D}^q = \bar{D}^\tilde{r}$. Now, if $(h_1, \ldots, h_k) \in \bar{D}$ with $y = \prod h_i$ then take $|y|$-multiple of $(h_1, \ldots, h_k)$ where $|y|$ denotes the order of $y$. This completes the proof of the claim.

\[\square\]

**5.3. Proof of Proposition 5.4.** Let $1 \leq e \leq d'$ with $(e, d') = 1$. Recall that the absolute Galois group $G_{\mathbb{F}_q}$ acts on the conjugacy classes $\mathcal{O}$ of $N$ as $\mathcal{O}_{\text{Frob}_q} = \mathcal{O}^q$ and the group $G$ acts on them via conjugation. Recall also that a Nielsen tuple $\bar{C}$ is called $\mathbb{F}_q$-rational of type $e$ if $\bar{C}^q = \bar{C}^{q^e}$, that is $\bar{C}^{q^e - e} = \bar{C}$. If we let $t_e = q^{e^r - e}$, then the cyclic group $T_e := \langle t_e \rangle$ generated by $t_e$ acts on Nielsen tuples. Given a conjugacy class $\mathcal{O}$, let $\mathcal{C}_e(\mathcal{O})$ be the $T_e$-orbit of $\mathcal{O}$. Obviously, the finite sum
\[ \tilde{\mathcal{O}}_e := \sum_{C \in \mathcal{C}_e(\mathcal{O})} C \]
is the “smallest” $\mathbb{F}_q$-rational Nielsen tuple of type $e$ containing the conjugacy class $\mathcal{O}$.

Likewise, we can consider the cyclic group $\tilde{T}_e = \langle q^{e^r - e} \rangle$, the $\tilde{T}_e$-orbit $\tilde{\mathcal{C}}_e(\tilde{\mathcal{O}})$ of a conjugacy class $\tilde{\mathcal{O}}$ of $\tilde{N}$ and define $\tilde{\mathcal{O}}_e := \sum_{C \in \tilde{\mathcal{C}}_e(\tilde{\mathcal{O}})} C$. Now, we are ready to prove our proposition.
Proof of Proposition 5.4. We want to prove the inequality on the left-hand-side.

Let $e$ be such that $1 \leq e \leq d'$ and $(e, d') = 1$. Let $\tilde{G}$, $\tilde{N}$ and $N'$ be as in Lemma 5.7 and let $\tilde{D}_1, \ldots, \tilde{D}_r$ be the Nielsen tuples in $\tilde{N}$ as in Lemma 5.8. For each conjugacy class $O$ in $N$ fix a conjugacy class $\tilde{O}$ in $\tilde{N}$ with $\pi(\tilde{O}) = O$. Note that $\pi(\tilde{O}_e) = b_0 \tilde{O}_e$ for some $b_0$. Given a Nielsen tuple $\tilde{C}$ in $\tilde{N}$ with $\tilde{C}' = \tilde{C}''e$, we can write $\tilde{C} = \sum_{\tilde{O}_e} a_{\tilde{O}_e} \tilde{O}_e$. The following Nielsen tuple in $\tilde{N}$

$$\tilde{D} := \sum_{\tilde{O}_e} \left[ \frac{a_{\tilde{O}}}{b_{\tilde{O}}} \right] \tilde{O}_e$$

is $\mathbb{F}_q$-rational of type $e$ and $\pi(\tilde{D}) = \tilde{C} + \tilde{C}'$ where $\tilde{C}'$ can be drawn from a finite set of Nielsen tuples $\tilde{C}_1', \ldots, \tilde{C}_s'$ with $\tilde{C}_i'^e = \tilde{C}_i'^{r_e}$ for all $i$.

Now, fix a Nielsen tuple $\tilde{B}$ in $\tilde{N}$ with $\tilde{B}'' = \tilde{B}^{'e}$ such that its projection $\pi'(\tilde{B})$ in $N'$ contains at least $c$ nontrivial conjugacy classes of $\tilde{N}$ where $c$ is the constant in Lemma 5.6. By Lemma 5.8, there exists an $i$ such that $\tilde{D} + \tilde{B} + \tilde{D}_i$ is $\mathbb{F}_{q'}$-rational of type $e$ and $\mathcal{H}^{\tilde{C}_i}_D + \tilde{B} + \tilde{D}_i(\mathbb{F}_q)$ is nonempty and, by Theorem 3.2, $\mathcal{H}^{\tilde{C}_i}_{D+B+D_i}$ defined over $\mathbb{F}_q$.

The projection $\pi(\tilde{D} + \tilde{B} + \tilde{D}_i)$ is $\mathbb{F}_{q'}$-rational of type $e$ and it can be expressed as $\tilde{C} + \tilde{C}_j + nI$ where $\tilde{C}_j$ can be drawn from a finite set of Nielsen tuples $\tilde{C}_1, \ldots, \tilde{C}_k$ and $I$ denotes the trivial conjugacy class. In other words, by Theorem 3.2, the scheme $\mathcal{H}^{\tilde{C}_j}_{\tilde{C} + \tilde{C}_j}$ is defined over $\mathbb{F}_q$.

We now claim that $\mathcal{H}^{\tilde{C}_j}_{\tilde{C} + \tilde{C}_j}$ has an $\mathbb{F}_q$-rational geometrically connected component. For any $\tilde{N}$-cover $Y \to \mathbb{P}^1$ we have the canonically associated $N$-cover $Y/U \to \mathbb{P}^1$ where $U := \ker(\pi : \tilde{N} \to N)$. This defines a morphism of schemes over $\mathbb{F}_q$

$$\pi_* : \mathcal{H}^{\tilde{C}_j}_{\tilde{C} + \tilde{C}_j} \to \mathcal{H}^{\tilde{C}_j}_{\tilde{C} + \tilde{C}_j}.$$

First of all, this implies that $\mathcal{H}^{\tilde{C}_j}_{\tilde{C} + \tilde{C}_j}(\mathbb{F}_q)$ is non-empty. Secondly, this map factors through (possibly over $\overline{\mathbb{F}}_q$) the natural map, which is induced likewise,

$$\pi'_* : \mathcal{H}^{\tilde{C}_j}_{\tilde{C} + \tilde{C}_j} \to \mathcal{H}^{\pi'(\tilde{C} + \tilde{C}_j)}_{\pi'(\tilde{D} + \tilde{B} + \tilde{D}_i)}.$$

Since $\pi'(\tilde{B})$ contains at least $\mathfrak{R}$ nontrivial conjugacy classes of $N'$, by Lemma 5.6, the image of $\pi'_*$ is geometrically connected and so is the image of $\pi_*$. The image of $\pi_*$ is the $\mathbb{F}_q$-rational geometrically connected component we want.

Define $h_2(q, \tilde{C})$ to be the number of $\mathbb{F}_{q'}$-rational geometrically connected components of $\mathcal{H}^{\tilde{C}}_D$ multiplied by $q^{|\tilde{C}|}$. By the discussion above, $h_2(q, \tilde{C} + \tilde{C}_j) \geq q^{|\tilde{C} + \tilde{C}_j|}$ for some $j$. For each $\mathbb{F}_{q'}$-rational Nielsen tuple $\tilde{C}$ of type $e$, fix such a $\tilde{C}_j$ and set $\tilde{C}^{pr} := \tilde{C} + \tilde{C}_j$.

Thus, we have

$$\sum_{\tilde{C}} h_2(q, \tilde{C}^{pr}) \geq \sum_{\tilde{C}} q^{|\tilde{C}^{pr}|} > \sum_{r < R} h_{ns}(q, r, e)$$

and

$$\sum_{\tilde{C}} h_2(q, \tilde{C}^{pr}) \leq \sum_{\tilde{C}} h_2(q, \tilde{C}) = \sum_{r < R + m} h_{cc}(q, r, e).$$
where \( m \) is the maximum of \( r(\bar{C}_j) \)'s and the sums run over \( \mathbb{F}_q \)-rational Nielsen tuples \( \bar{C} \) of type \( e \). This completes the proof.

### 5.4. Proof of Theorem 1.2

In this section, our main purpose is to prove Theorem 1.2; that is, to prove:

**Theorem 5.9.** Assume that \( (q, |G|) = 1 \) and that \( G = N \rtimes T \). Then, we have

\[
\mathcal{Z}_{N,G}(\mathbb{F}_q, X) \asymp X^a(N) (\log X)^{b(N,G,F_q)-1}.
\]

Below, we define the constant \( b(N,G,F_q) \) and prove Theorem 5.9. We need the following lemma from Tauberian theory, for a proof see [10, Lemma 2.3]:

**Lemma 5.10.** Suppose \( \{a_n\} \) is a sequence of real numbers with \( a_n = 0 \) whenever \( n \) is not a power of \( q \), and suppose

\[
\sum_{r=1}^{\infty} a_{q^r} q^{-rs}
\]

considered as a formal power series, is a rational function \( f(t) \) of \( t = q^s \). Let \( a \) be a positive real number. If \( f(t) \) has no poles with \( |t| \geq q^a \), then

\[
\sum_{n=1}^{X} a_n \ll X^a.
\]

If \( f(t) \) has a pole of order \( b \) at \( t = q^a \) and no other poles with \( |t| \geq q^a \), then

\[
\sum_{n=1}^{X} a_n \asymp X^a (\log X)^{b-1}.
\]

Let \( 1 \leq e \leq d' \) with \( (e, d') = 1 \). Given a conjugacy class \( O \) in \( N \), let \( C_e(O) \) denote its \( T_e \)-orbit and let \( \bar{O}_e := \sum_{\bar{C} \in C_e(O)} \bar{C} \). Let \( d' = |G/NH| = |T'| \). Denote the set of \( N \)-conjugacy classes of minimal-index elements of \( N \) by \( \mathcal{C}(N) \). Define

\[
C_e(N, G, \mathbb{F}_q) := \{ \bar{O}_e : O \in \mathcal{C}(N) \} \quad \text{and} \quad b_e(N, G, \mathbb{F}_q) := |C_e(N, G, \mathbb{F}_q)|.
\]

Finally, set

\[
b(N, G, \mathbb{F}_q) = \max \{b_e(N, G, \mathbb{F}_q) | 1 \leq e \leq d' \text{ and } (e, d') = 1 \}.
\]

Note that

\[
C_e(N, G, \mathbb{F}_q) = \mathcal{C}(N)/G_{\mathbb{F}_q}
\]

is in fact the set of \( G_{\mathbb{F}_q} \)-orbits on \( \mathcal{C}(N) \), where \( G_{\mathbb{F}_q} \)-action in consideration is defined via \( \zeta_e \)-twisted cyclotomic character – \( \zeta_e \in H^1(\mathbb{F}_q, T') \).

**Proof of Theorem 5.9.** By Proposition 5.4, we have

\[
\sum_{q^r < X} h_{cc}(q, r) \asymp \sum_{q^r < X} h_{ns}(q, r) = \sum_{1 \leq e \leq d'} \sum_{q^r < X} h_{ns}(q, r, e).
\]

On the other hand, for every \( e \) with \( 1 \leq e \leq d' \) and \( (e, d') = 1 \), we have the factorization:

\[
\sum_{r=1}^{\infty} h_{ns}(q, r, e) q^{-rs} = \sum_{\bar{C}} q^{\bar{C}|q^{-r(\bar{C})s}} = \prod_{\bar{O}_e} \frac{1}{1 - q^{\bar{O}_e s(1 - \text{ind}(\bar{O}_e)s)}}
\]
where the product is indexed by $T_e$-orbits $\bar{O}_e$ of conjugacy classes $O$ of $N$, $\text{ind}(\bar{O}_e)$ is the index of an element of $O$ and $|\bar{O}_e|$ denotes the number of conjugacy classes in the orbit $\bar{O}_e$. We see that the series $\sum_{r=1}^{\infty} h_{ns}(q, r, e)q^{-rs}$ has a pole at $s = a(N)$ of order $b_e(N, G, F_q)$ and no other poles for $s > a(N)$. By Lemma 5.10,

$$\sum_{q^r < X} h_{ns}(q, r, e) \asymp X^{a(N)}(\log X)^{b_e(N, G, F_q) - 1}$$

and so

$$\sum_{1 \leq e \leq d'} \sum_{q^r < X \atop (e,d')=1} h_{ns}(q, r, e) \asymp X^{a(N)}(\log X)^{b(N, G, F_q) - 1}$$

for sufficiently large $X$. Putting them all together, we get

$$\sum_{q^r < X} h_{cc}(q, r) \asymp X^{a(N)}(\log X)^{b(N, G, F_q) - 1}$$

and this completes the proof.

6. Proof of Theorem 1.4 and the Corollaries

Below, we prove Theorem 1.4, write a conjecture for the counting function $Z_G(\mathfrak{K}, X)$ for any global field $\mathfrak{K}$ and, using Theorem 1.4, we show that our conjecture gives the right asymptotic in some important cases.

By Theorem 3.2, $Z_{N,G}(F_q, X)$ is asymptotic to $\sum_{q^r < X} h_G(q, r)$. On the other hand, by Proposition 4.2, we have $\sum_{q^r < X} h_G(q, r) \asymp \sum_{q^r < X} h_N(q, r)$. Thus, we get:

Lemma 6.1. We have

$$Z_{N,G}(F_q, X) \asymp \sum_{q^r < X} h_N(q, r).$$

Recall that $Z'_{N,G}(F_q, X) = \sum_{q^r < X} h_{cc}(q, r)$. Observe that Heuristic 1.3 implies that $h_N(q, r) = h_{cc}(q, r)$ (this is indeed the only point where we use the heuristic). So, by Lemma 6.1, $Z_{N,G}(F_q, X)$ has the same asymptotic order with the counting function $Z'_{N,G}(F_q, X)$ on heuristic grounds. More precisely, we have:

Lemma 6.2. Assume Heuristic 1.3. If $G = N \rtimes T$, then we have

$$Z_{N,G}(F_q, X) \asymp Z'_{N,G}(F_q, X).$$

Now, Theorem 1.4 immediately follows from Theorem 5.9.

6.1. Examples and corollaries. As a special case, we get the result of Ellenberg-Venkatesh [10]:

Corollary 6.3. If $(q, |G|) = 1$, then $Z'_{G,G}(F_q, X) \asymp X^{a(G)}(\log X)^{b(G, F_q) - 1}$.

Proof. We just need to show that $b(G, G, F_q) = b(G, F_q)$. Using the notation above, we have $d = e = 1$ and $\tau = 1$ in $G$. So, $C_e(G, G, F_q) = C(G)/G_{F_q}$ and $b(G, G, F_q) = b_e(N, G, F_q) = |C(G)/G_{F_q}| = b(G, F_q).$ $\square$
Let $G = (((123)) \oplus ((456))) \times ((14)(25)(36)) \leq S_6$ and let $Z_G(Q, Q(\zeta_3), X)$ be the number of isomorphism classes of $G$-extensions $\mathcal{R}/\mathbb{Q}$ containing $Q(\zeta_3)$ such that $\Delta(\mathcal{R}/\mathbb{Q}) < X$. In [15], Klüners shows that $Z_G(Q, X) \asymp X^{1/2} \log X$ contradicting with Malle’s conjecture which predicts $Z_G(Q, X) \asymp X^{1/2}$. Indeed, he proves that $Z_G(Q, Q(\zeta_3), X) \asymp X^{1/2} \log X$. With evident modifications, one gets the same result in function field case for $q = 2 \pmod{3}$ i.e. $Z_G(\mathbb{F}_q, \mathbb{F}_q^2, X) \asymp X^{1/2} \log X$. The following corollary shows that our theorem gives the right asymptotic for the number of $G$-extensions in this case (provided with the Heuristic).

**Corollary 6.4.** If $(q, |G|) = 1$, then $Z'_G(\mathbb{F}_q, X) \asymp X^{1/2} \log X$ where $G = (((123)) \oplus ((456))) \times ((14)(25)(36))$ and $q = 2 \pmod{3}$.

**Proof.** Given an $G$-extension $\mathcal{R}/\mathbb{F}_q(t)$, maximal constant intermediate subfield in its Galois closure $\overline{\mathcal{R}}/\mathbb{F}_q(t)$ might be $\mathbb{F}_q(t)$, $\mathbb{F}_q^2(t)$ or $\mathbb{F}_q^e(t)$ corresponding to the normal subgroups of $G$, respectively, $G, G_1 := \langle (123) \rangle \oplus \langle (456) \rangle$ or $G_2 := \langle (123)(456) \rangle$. Therefore, we have

$$Z'_N(\mathbb{F}_q(t), X) \asymp Z'_{G,G}(\mathbb{F}_q, X) + Z'_{G_1,G}(\mathbb{F}_q, X) + Z'_{G_2,G}(\mathbb{F}_q, X).$$

Using Theorem 1.2, one can easily see that

$$Z'_{G,G}(\mathbb{F}_q, X) \asymp X^{1/2} \quad \text{and} \quad Z'_{G_2,G}(\mathbb{F}_q, X) \asymp X^{1/4}.$$

We will show that $Z'_{G_1,G}(\mathbb{F}_q, X) \asymp X^{1/2} \log X$. Using the notation above, we have:

$$\mathcal{C}(G_1) = \{(123), (132), (456), (465)\},$$

$a(N) = 1/2, d = d' = 2, e = 1$ and $\tau = (14)(25)(36)$. We have two $T_e$-orbits: $\{(123), (465)\}$ and $\{(132), (456)\}$. Therefore, $b(G_1, G, \mathbb{F}_q) = b_0(G_1, G, \mathbb{F}_q) = 2$. QED.

Another interesting example in [15] is $G \cong (C_3 \wr C_3) \times C_2 \subseteq S_{18}$ where $C_3$ denotes the cyclic group of order 3. Klüners shows that $Z_G(\mathbb{Q}, X) \ll X^{1/4}$. In function field case, our main result gives us the asymptotic predicted by Klüners:

**Corollary 6.5.** If $(q, |G|) = 1$, then $Z'_G(\mathbb{F}_q(t), X) \asymp X^{1/4}$ where $q = 2 \pmod{3}$ and $G \cong (C_3 \wr C_3) \times C_2 \subseteq S_{18}$.

**Proof.** Let’s write $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \langle g_3 \rangle \times \langle x \rangle \times \langle y \rangle$. We will just consider the normal subgroups $N$ with $a(N) = a(G)$. Given a $G$-extension $\mathcal{R}/\mathbb{F}_q(t)$, $G$ has four such normal subgroups $N$ with cyclic quotient corresponding to possible maximal constant subextensions in the Galois closure of $\mathcal{R}/\mathbb{F}_q(t)$. So, we have four cases.

**Case 1:** $N = G$. In this case, $\mathcal{C}(N) = \{g_1, g_1^2\}$ where $g_i$ denotes the conjugacy class of $g_i$. So, $a(G) = 1/4$. Since $q = 2 \pmod{3}$ and $d = d' = e = 1$, there is only one $T_e$-orbit, namely $\{g_1, g_1^2\}$. Thus, $b(G, G, \mathbb{F}_q) = 1$ and $Z'_{N,G}(\mathbb{F}_q, X) \asymp X^{1/4}$.

**Case 2:** $N = C_3 \wr C_3$. We have $|G : N| = 2$, $a(N) = 1/4$ and $d' = e = 1$ since $y \in \text{Cen}_G N$. With the notation above, we have $\tau = y$ and $\mathcal{C}(N) = \{g_1, g_1^2\}$. Since $\tau \in \text{Cen}_G N$, the only $T_e$-orbit is $\{g_1, g_1^2\}$ and so $b(N, G, \mathbb{F}_q) = 1$. Hence, $Z'_{N,G}(\mathbb{F}_q, X) \asymp X^{1/4}$.

**Case 3:** $N = C_3 \times C_3 \times C_3$. We have $|G : N| = 6$, $a(N) = 1/4$, $d' = 3$ and $\tau = xy$. We have $\mathcal{C}(N) = \{g_1, g_1^2, g_2, g_2^2, g_3, g_3^2\}$ and $e = 1$ or $e = 2$. One can easily see

$$C_1(g_i^e) = C_2(g_i^e) = \{g_1, g_1^2, g_2, g_2^2, g_3, g_3^2\}$$

for $i = 1, 2, 3$ and $e = 1, 2$. Therefore, there is only one $T_e$-orbit and $b(N, G, \mathbb{F}_q) = 1$. Hence, $Z'_{N,G}(\mathbb{F}_q, X) \asymp X^{1/4}$.

**Case 4:** $N = C_3 \times C_3 \times C_3 \times C_2$. Using the same argument in the previous case, we see that $Z'_{N,G}(\mathbb{F}_q, X) \asymp X^{1/4}$. QED.
The following corollary shows that our result, Theorem 1.4, is consistent with Wright's result [22] where he proves Malle's conjecture for abelian groups when the base field is $\mathbb{Q}$. To show that it is consistent, we need to prove that there are “more” extensions without a constant subextension than the ones with a constant subextension (whose corresponding subgroup is $N$). In other words, by Corollary 6.3 and Lemma 6.2, it is enough to prove the following.

**Corollary 6.6.** Let $G$ be an abelian group and $(q, |G|) = 1$. Then, $Z'_{N,G}(\mathbb{F}_q, X) \ll Z'_{G,G}(\mathbb{F}_q, X)$ for any normal subgroup $N$ with a cyclic complement.

**Proof.** Let $N$ be such a subgroup. Then, $a(N) \leq a(G)$. If $a(N) < a(G)$, then we are done. Assume that $a(N) = a(G)$. Since $G$ is abelian, $d' = e = 1$ and $C_1(N,G, \mathbb{F}_q) = C(N)/G_{\mathbb{F}_q}$. On the other hand, $C(G,G,\mathbb{F}_q) = C(G)/G_{\mathbb{F}_q}$ and $C(N) \subseteq C(G)$. So, $b(N,G,\mathbb{F}_q) \leq b(G,G,\mathbb{F}_q)$ and we are done. \[\square\]

### 6.2. Refined Malle’s conjecture

Note that one can revise Malle’s conjecture (in other words, the constant $b(G,\mathbb{F}_q)$ in the conjecture) for function fields by just taking the maximum of all the constants $b(N,G,\mathbb{F}_q)$ over all normal subgroups $N \leq G$ with cyclic quotient and $a(N) = a(G)$. Notice that the constant $b(N,G,\mathbb{F}_q)$ is defined for any such subgroup $N$ (which does not necessarily have a complement $T$ in $G$).

Now, we want to conclude our paper with the statement of the revised conjecture in number field case. First, we will introduce some notation. Let $\mathfrak{K}$ be a number field. We need to consider normal subgroups $N \leq G$ with abelian quotient $G/N$. Let $\mathfrak{K}^c$ be the maximal cyclotomic extension of $\mathfrak{K}$ (in a fixed algebraic closure $\overline{\mathfrak{K}}$). Given a cocycle $\varphi \in \text{Hom}(G(\mathfrak{K}^c/\mathfrak{K}), G/N)$ and a conjugacy class $\tilde{g}$ in $N$, define $\varphi$-twisted action of $\sigma \in G_{\mathfrak{K}}$ on $\tilde{g}$ by

$$
\sigma(\tilde{g}) := \tilde{g}\chi(\varphi(\text{Res}(\sigma)))^{-1}
$$

where $\text{Res} : G_{\mathfrak{K}} \to G(\mathfrak{K}^c/\mathfrak{K})$ is the restriction, $\chi$ is the cyclotomic character and $\varphi(\text{Res}(\sigma))^{-1}$ acts on the conjugacy class by conjugation. By analogy, we define

$$
b_\varphi(N,G,\mathfrak{K}) := |C(N)/G_{\mathfrak{K}}|
$$

where the $G_{\mathfrak{K}}$-action in question is the $\varphi$-twisted action. Finally, set

$$
b(N,G,\mathfrak{K}) = \max\{b_\varphi(N,G,\mathfrak{K}) : \varphi \in \text{Hom}(G(\mathfrak{K}^c/\mathfrak{K}), G/N) \text{ and } \varphi \text{ is surjective}\}.
$$

In case there is no surjective homomorphism $\varphi \in \text{Hom}(N(\mathfrak{K}^c/\mathfrak{K}), G/N)$, we take $b(N,G,\mathfrak{K}) = 0$ as the convention. Based on our result, we propose the following correction to Malle’s conjecture for any finite transitive subgroup $G \subseteq S_n$:

**Conjecture 6.7.** Fixing $G$ and $\mathfrak{K}$, set

$$
b(G,\mathfrak{K}) = \max\{b(N,G,\mathfrak{K}) : G/N \text{ is abelian, and } a(N) = a(G)\}.
$$

Then, we have

$$
Z_G(\mathfrak{K}, X) \asymp X^{a(G)}(\log X)^{b(G,\mathfrak{K})-1}.
$$

We remark that there are counterexamples in [15] which are different than the one in Corollary 6.4, but in the same spirit. Using Theorem 1.4, one can show that our result gives the right asymptotic in these cases.
Summing it up, in the case of function fields, corollaries of our result shows that the conjecture above coincides with the existing results on Malle’s conjecture and eliminates all the counterexamples known (to our knowledge) so far. Hence, it provides strong evidence in favor of the conjecture above.

6.3. A remark on Heuristic 1.3. As mentioned in the introduction of section 6, Heuristic 1.3 implies the equality of the counting functions $h_N(q, r) = h_{cc}(q, r)$ and this in turn implies the fact in Lemma 6.2 that $Z_{N,G}(\mathbb{F}_q, X) \simeq Z_{N,G}^t(\mathbb{F}_q, X)$. This is the only point where we use the heuristic. Notice that we only need that $h_N(q, r) \approx h_{cc}(q, r)$ to prove Lemma 6.2 (rather than the equality $h_N(q, r) = h_{cc}(q, r)$).

In order to show that $h_N(q, r) \approx h_{cc}(q, r)$, it suffices to have a formula (with a good error term) for the number of geometrically connected components $H_d$ of $H_G/\mathbb{F}_q$ of dimension $d$, such as

\[(10) \quad |H_d(\mathbb{F}_q)| = c(q)q^d + \text{Error}(d)\]

where $c(q)$ is a constant that approaches to 1 as $q$ approaches to infinity. Note that, in equation (10), the dimension $d$ grows and $q$ is fixed. In fact, it is enough to have the equality (10) for geometrically connected components $H_d/\mathbb{F}_q$ with sufficiently big dimension as we are only interested in the asymptotics. To our knowledge, there is no general conjecture for the error term. This, with avoiding the technicality, is one of the reasons that we don’t assume a more valid heuristic to prove our results. Instead, we isolate the use of Heuristic 1.3 in Lemma 6.2.

Although there is no general conjecture on the error term, it seems reasonable to expect the error term to be $O(q^{d(1-\epsilon(N))})$ where $\epsilon(N)$ is a positive constant depending only on the group $N$. For instance, let $N = S_3$ and $C_d = (\tau, ..., \tau)$ be the $d$-tuple of the conjugacy class $\tau$ of transpositions. It is known that $H_d$ is geometrically connected when $d = \dim H_d$ is sufficiently big, a result due to Hurwitz [13]. For $H_d = H_d^c$, the expected error term is $O(q^{d(1-1/6)})$.

By Lefschetz fixed point formula, calculating $|H_d(\mathbb{F}_q)|$ boils down to computing the trace of the Frobenius on $\ell$-adic cohomology spaces $H^i_{et}(H_d \times_{\mathbb{F}_q} \mathbb{F}_q, \mathbb{Q}_\ell)$. More precisely, if one shows that there exists a constant $A$ such that

\[(11) \quad \dim H^i_{et}(H_d \times_{\mathbb{F}_q} \mathbb{F}_q, \mathbb{Q}_\ell) \leq A^i\]

for all $d, i \geq 1$, then one gets:

\[-\frac{1}{\sqrt{q}/A - 1} \leq \frac{|H_d(\mathbb{F}_q)|}{q^d} - 1 \leq \frac{1}{\sqrt{q}/A - 1},\]

see [11, Section 1.7]. In other words, such an upper bound on the dimension of the cohomology group implies that $|H_d(\mathbb{F}_q)|$ is about $q^d$.

In a recent preprint [11], Ellenberg-Venkatesh-Westerland was able to get an upper bound as in (11) for the subschemes $H_d = H_d^c$ of $H_G/\mathbb{F}_q$, for a special class of groups $N$ including the dihedral groups and Nielsen tuples $C_d = (C, ..., C)$ – a $d$-tuple of a conjugacy class $C$. More precisely, they show that, given a group $N$ and conjugacy class $C$ satisfying certain technical condition, there exists constants $A = A(N, C), B = B(N, C)$, depending only on $N$ and $C$, such that

\[
\dim H^i_{et}(H_d \times_{\mathbb{F}_q} \mathbb{F}_q, \mathbb{Q}_\ell) < BA^i
\]

for all $i, d$, see [11, Proposition 7.6].
Although we are far from proving the formula (10) with the error term $O(q^{d(1-\epsilon)})$, the recent result of Ellenberg-Venkatesh-Westerland shows that it is very reasonable to expect such an equality. Nevertheless, given a formula as in (10) with a good error term, one can modify our argument by proving Lemma 6.2. In summary, we believe that our result will prove its use in time as we know more about the number of $\mathbb{F}_q$-rational points on $\mathcal{H}_N/\mathbb{F}_q$.

References

[1] M. Bhargava. The density of discriminants of quartic rings and fields, *Ann. of Math.*, 162, 1031-1063, 2005.
[2] M. Bhargava. The density of discriminants of quintic rings and fields, *Ann. of Math.* 172.3 , 1559-159, 2010.
[3] A. Cadoret. Galois categories. In *Arithmetic and geometry around Galois Theory*. Vol. 304. Springer, 2012.
[4] A. Clebsch. Zur Theorie der Riemann’schen Flächen. Math. Ann. 6:216-230, 1872.
[5] H. Cohen, F. Diaz y Diaz and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$, Compositio Math. 133 , 65-93, 2002.
[6] H. Davenport and H. A. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A.* 322(1551):405-420, 1971.
[7] P. Debes and G. C. Doual. Algebraic Covers: field of moduli versus field of definition. *Ann. Sci. Ecole Norm. Sup. (4)*, 30 , no. 3, p 303-338, 1997.
[8] B. Datskovsky and D. G. Wright. Density of discriminants of cubic extensions, *G. Reine Angew. Math.* 386, 116-138, 1998.
[9] G. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant, *Ann. of Math.* 163 (2), 723–741, 2006.
[10] G. Ellenberg and A. Venkatesh. Counting extensions of function fields with bounded discriminant and specified Galois group. In *Geometric Methods in Algebra and Number Theory*, volume 235 in *Progress in Mathematics*, pages 151-168. Birkhauser, 2005.
[11] G. Ellenberg, A. Venkatesh and C. Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, Preprint, 2009.
[12] M. D. Fried and H. Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.,* Volume: 290, no. 4, p. 2021-2027, 1991.
[13] A. Hurwitz. Über Riemann’sche Flächen mit gegebenen Verzweigungspunkten. Math. Ann. 39:1-61, 1891.
[14] G. Klüners and N. Malle. Counting nilpotent Galois extensions. *G. Reine. Angew. Math.*, 572:1-26, 2004.
[15] G. Klüners. A Counter Example to Malle’s Conjecture on the Asymptotics of Discriminants, *C. R. Acad. Sci. Paris, Ser. I* 340, 2005.
[16] N. Malle. On the distribution of Galois groups. *G. Number Theory*, Volume: 92, no. 2, p. 315-329, 2002.
[17] N. Malle. On the distribution of Galois groups II. *Exp. Math.*, 13:129-135, 2004.
[18] N. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer-verlag, 1999.
[19] A. Grothendieck. Revetements Etales et Groupe Fondamental (SGA 1), LNM 224, Springer, 1971.
[20] A. Tamagawa. Fundamental groups and geometry of curves in positive characteristic, *In Arithmetic fundamental groups and noncommutative algebra*, volume 70 in *Proceedings of symposia in pure mathematics*, 1999.
[21] S. Wewers. Construction of Hurwitz spaces. PhD Thesis, University Essen, 1998.
[22] D. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.*, 58:17-50, 1989.
DEPARTMENT OF MATHEMATICS, WESTERN ILLINOIS UNIVERSITY, MACOMB, IL, USA, 61455

E-mail address: s-turkelli@wiu.edu