Counterexamples for Türkelli's Modification on Malle's Conjecture

Jiuya Wang

October 15, 2024

Abstract

We give counterexamples for the modification on Malle's Conjecture given by Türkelli. Türkelli's modification on Malle's conjecture is inspired by an analogue of Malle's conjecture on function field. As a byproduct, our counterexamples show that the b constant can be different between function field and number field. Along the same line, we also show that Klüner's counterexamples give counterexamples for a natural extension of Malle's conjecture on counting number fields by product of ramified primes.

Key words. Malle's conjecture, roots of unity, cyclotomic extension, embedding problem

1 Introduction

1.1 Malle's Conjecture

It is a standard result in algebraic number theory that there are finitely many number fields with bounded discriminant. It is then natural to ask how many number fields there are with bounded discriminant. Malle [Mal02, Mal04] gives a conjectural asymptotic answer for this question. For each number field F/k with degree n, we define the permutation Galois group $\mathrm{Gal}(F/k)$ to be the image of G_k in S_n induced by G_k action on embeddings of F into $\bar{k}$. Given a transitive group $G \subset S_n$, we denote $N_k(G, X)$ to be the number of subfields $F \subset \bar{k}$ with $\mathrm{Gal}(F/k) = G$ with relative discriminant $\mathrm{Nm}_{k/\mathbb{Q}}(\mathrm{disc}(F/k)) \leq X$. The conjecture states:

Conjecture 1 (Malle's conjecture over Number Fields, [Mal02, Mal04])**.** *Given a number field k and a transitive permutation group $G \subset S_n$. There exists positive constants $C(G,k)$, $a(G) \in \mathbb{Z}$ and $b_M(G,k) \in \mathbb{Z}$ such that*

$$N_k(G, X) \sim C(G,k) X^{1/a(G)} \log^{b_M(G,k)-1} X. \tag{1.1}$$

Malle also gives a precise conjectural value for $a(G)$ in [Mal02] and for $b_M(G,k)$ in [Mal04], see Section 2 for precise description of Malle's proposed constants. Here we use the subscript in $b_M(G,k)$ to distinguish it from the true value $b(G,k)$ for powers of $\ln X$.

Progresses have been made towards this conjecture[Wri89, DH71, DW88, Bha05, Bha10, Klü12, Klü05b, CyDO02, Wan21, MTTW20, BW08, BF10, KP21, KW21]. The integer $a(G)$ has been widely believed to be true. In all cases towards Conjecture 1 where the asymptotic distribution for $N_k(G, X)$ is determined, the true value matches the conjectural $a(G)$. Conjecture 1 is also sometimes termed as *strong Malle's Conjecture*, in contrast to the *weak Malle's Conjecture* where $N_k(G, X)$ is predicted to be bounded between $X^{1/a(G)}$ and $X^{1/a(G)+\epsilon}$ asymptotically.

Recently, work of Ellenberg-Tran-Westerland [ETW17] proves the upper bound in weak Malle's conjecture for every permutation group G over global function field $k = \mathbb{F}_q(t)$ with large q relatively prime to $|G|$, which gives a strong evidence towards the validity of $a(G)$. Klüners and the author show that the upper bound in weak Malle's conjecture over number fields is equivalent to the discriminant multiplicity conjecture in general, and the latter is proved for all nilpotent permutation groups in [KW21]. For solvable groups, the discriminant multiplicity conjecture is simply equivalent to ℓ-torsion conjecture, and the latter is shown to be a consequence of a much weakened version of Cohen-Lenstra type heuristics [PTBW19].

The integer $b(G,k)$ is more mysterious. In 2005, Klüners [Klü05a] gives counterexamples to Conjecture 1 by noticing that certain intermediate cyclotomic extensions can contribute larger exponent for $\ln X$ than Malle's prediction $b_M(G,k)$. Among these counterexamples of similar spirit, the most famous one is the wreath product $C_3 \wr C_2$: it is noticed that the number of $C_3 \wr C_2$-extensions containing the cyclotomic field $\mathbb{Q}(\mu_3)$ is already contributing higher powers of $\ln X$ than $b_M(G,\mathbb{Q})$. Klüners also show the correct value $b(G,\mathbb{Q})$ for this example. Essentially, due the presence of intermediate cyclotomic extensions, one can follow the same construction to show that Conjecture 1 is inconsistent with itself in general, without proving any distribution.

1.2 Türkelli's Modification: inspiration and comparison with function fields

Like many problems in number theory, we can study the counterparts over global function field. Conjecture 1 over global function fields can be stated in a similar way (see Section 2 for explanations on why we do not conjecture an asymptotic distribution). We state the Malle's conjecture for global function field, exactly as how [Tür15, Conjecture 1.1] formulates it:

Conjecture 2 (Malle's Conjecture over Function Field)**.** *Given a global function field Q and a transitive permutation group $G \subset S_n$ with $(|G|, ch(Q)) = 1$. Define $a(G)$ and $b_M(G,Q)$ as in Conjecture 1. Then*

$$N_Q(G,X) = \Theta(X^{1/a(G)} \ln^{b_M(G,Q)-1} X). \tag{1.2}$$

Klüner's counterexamples also hold over global function fields if we allow constant extensions contained in G-extensions.

In order to accommodate these counterexamples, Türkelli in [Tür15] gives a modification of Conjecture 1 by proposing a new b-constant $b_T(G,Q)$ for both function fields and number fields, see Section 2.2 for the description.

Conjecture 3 (Türkelli's Modification [Tür15])**.** *Given a transitive permutation group $G \subset S_n$ and a global field Q with $(|G|, ch(Q)) = 1$,*

$$b(G,Q) = b_T(G,Q). \tag{1.3}$$

It is based on an extension of Ellenberg-Venkatesh's heuristic argument, where $b(G,Q)$ is related to the number of geometrically connected components of Hurwitz spaces and both $a(G)$ and $b_M(G,Q)$ are shown to match the true counting function when enumerating extensions without constant fields [EV05] (under the heuristic). Türkelli's new input is to consider G-extensions L/Q with the fixed subfield L^N being exactly the maximal constant extensions contained in G. This extension of heuristics then leads to a conjectural distribution for such L, given explicity in [Tür15]. It is then natural that on the function field side the modification is to take the sum over all possible constant extensions. To translate the problem to number fields, Türkelli simply

consider the sum of his heuristic distribution over all possible abelian extensions with Galois group a quotient of G.

In this paper, we give counterexamples for Conjecture 3 in Theorem 1.3. We demonstrate the key idea via a simple example:

Example 1.1. *Let* $G = C_3 \wr C_4 \subset S_{12}$ *and* $\gcd(q, |G|) = 1$. *We have*

$$b_T(G, \mathbb{Q}) = b(G, \mathbb{F}_q(t)) = 2, \qquad b(G, \mathbb{Q}) = b_M(G, \mathbb{Q}) = 1.$$

With C_4 in place of C_2 in Klüner's counterexample has forbidden the existence of the cyclotomic field$\mathbb{Q}(\mu_3)$ as an intermediate extension over $\mathbb{Q}$. We now make a couple comments on this example. Firstly, it is probably surprising that in this example the prediction of Malle is correct whereas the the modification of Türkelli is not! Secondly and more importantly, even when a number field and a global function field have the same relevant cyclotomic extension $\mathrm{Gal}(Q(\mu_d)/Q)$ for d determined by G, it can happen that the b-constants are different! Thirdly, when $\mathrm{Gal}(Q(\mu_d)/Q)$ are the same, it seems that there exist more field extensions on function field side.

We now demonstrate the reasoning behind the example and the last comment more carefully. Given a finite group G and G/N a quotient group, the study of whether a particular G/N-extension can be embedded to a G-extension is called *embedding problem*. It is a study with rich history and theory, and historically play a central role in solving inverse Galois problem for solvable groups. A particular embedding problem becomes necessary in studying $b(G, k)$ in Conjecture 1: given a fixed cyclotomic extension, i.e., $k(\mu_n)$ with $\mathrm{Gal}(k(\mu_n)/k)$ being a quotient of G, can $k(\mu_n)$ be embedded into a G-extension. We formulate precisely the following question:

Question 1.2 (Embedding Cyclotomic Extensions)**.** *Let* Q *be a global field. Given a surjective group homomorphism* $\pi : G \to B$ *and a cyclotomic* B*-extension* F/Q *(equivalently a surjective continous group homomorphism* $\phi : G_Q \to B$ *that factors through), does there exists a surjective* $\tilde{\phi} : G_Q \to G$ *such that* $\tilde{\phi} \circ \pi = \phi$*?*

$$\begin{array}{ccccccccc} & & & & & & G_Q & & \\ & & & & & \swarrow^{\tilde{\phi}} & \downarrow \phi & & \\ 0 & \longrightarrow & \mathrm{Ker}(\pi) & \longrightarrow & G & \xrightarrow{\pi} & B & \longrightarrow & 0 \end{array}$$

In Example 1.1, we can easily see that an C_4-extension cannot contain $\mathbb{Q}(\mu_3)$ because one encounter both local obstructions at $p = 3$ and $p = \infty$. It seems quite difficult to solve this problem in full generality. We will discuss some cases in Section 4, which suffices for proving the following theorem, giving an infinite family of examples where $b(G, \mathbb{Q})$ is bounded between $b_T(G, \mathbb{Q})$ and $b_M(G, \mathbb{Q})$.

Theorem 1.3. *Let* ℓ *be an odd prime number and* $d = \prod_i p_i^{r_i} \neq 2$ *where* p_i *are all prime numbers. Let* $G = C_\ell \wr C_d \subset S_{\ell d}$ *with* $(|G|, ch(Q)) = 1$ *and* $\mathrm{Gal}(\mathbb{F}_q(t)(\mu_\ell)/\mathbb{F}_q(t)) = Gal(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. *Denote* $\gcd(d, \ell - 1) = \prod_i p_i^{s_i}$. *Let* $s = val_2(\ell - 1) - 1$ *when* $val_2(d) > val_2(\ell - 1)$ *and* $s = 0$ *otherwise. Then*

$$b_T(G, \mathbb{Q}) = b(G, \mathbb{F}_q(t)) = \prod_i p_i^{s_i}, \quad b(G, \mathbb{Q}) = \prod_{i, r_i = s_i} p_i^{s_i} \cdot 2^s, \quad b_M(G, \mathbb{Q}) = 1.$$

In particular, there exists $G \subset S_n$ *such that* $\mathrm{Gal}(\mathbb{F}_q(t)(\mu_\ell)/\mathbb{F}_q(t)) = \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ *and* $b(G, \mathbb{F}_q(t)) > b(G, \mathbb{Q})$.

We exclude $d = 2$ only because $b(G, \mathbb{Q})$ is not proved over number field currently due to lack of good ℓ-torsion bound. One can construct more examples along this line, either in wreath product or non-wreath product. We don't try to expand in that direction here. Theorem 1.3 provides family of infinite examples that are simple as groups, and also indicates the robustness in the comments we make after Example 1.1. Therefore we make the following conjecture:

Conjecture 4. *Let k be a number field. Then for any transitive permutation group G, we have*

$$b_M(G, k) \leq b(G, k) \leq b_T(G, k). \tag{1.4}$$

It is worth mentioning that at this moment, the issue from embedding problem in Türkelli's modification seems to only exist for number fields. We are not aware of any counterexamples over function fields, either for Conjecture 3 or Problem 1.2. Given Theorem 4.1, it seems to be plausible to expect we don't have such failures for Problem 1.2 over function field. Though a positive answer in full generality seems to be difficult to prove.

1.3 General Invariants

Malle's conjecture is also interesting because of its connection to other asymptotic questions. In fact, field enumeration naturally occurs when one studies statistical questions for all G-extensions as a family. For example, it is exactly the denominator appearing in Cohen-Lenstra type heuristics. Choosing the ordering for field enumeration is important from this perspective. It has been noticed that ordering field by discriminants does not always produce the predicted average number from Cohen-Martinet heuristics , e.g. $G = \mathbb{Z}/4\mathbb{Z}$ [BLJ20]. In fact, this phenomena already exists for $G = D_4$ in [CyDO02] and Klüners examples of wreath product [Klü05a]. To avoid such problems, people have worked in the past with conductor or product of ramified primes [Woo10, ASVW21]. It is suggested first in [Woo10] to use product of ramified primes as the counting invariant and is conjectured by [BLJ20] that it is always good for the purpose of Cohen-Lenstra heuristics, and is actually used [LWZB19] on Cohen-Lenstra heuristics over function fields for general Galois groups. With notations introduced in 2, it naturally extends Conjecture 1

Conjecture 5 (Generalized Malle's Conjecture)**.** *Given a global function field Q and a transitive permutation group $G \subset S_n$ with $(|G|, ch(Q)) = 1$. Let inv be a counting invariant(see Definition 2.1). Then there exists positive constants $a(G^{inv}) \in \mathbb{Z}$ and $b(G^{inv}, Q) \in Z$ such that*

$$N_Q(G^{inv}, X) = \Theta(X^{1/a(G^{inv})} \ln^{b(G^{inv},Q)-1} X),$$

where $b(G^{inv}, Q) = b_M(G^{inv}, Q)$.

The reason for aforementioned issue is very often concluded to be the following group theoretic reason. In the upcoming paper of the author with Alberts, Lemke-Oliver and Wood, we define *concentrated* groups, to capture this feature:

Definition 1.4 (Concentrated Group, [AOWW24])**.** *We say a transitive permutation group $G \subset S_n$ is* concentrated*, or* concentrated in N*, if there exists a proper normal subgroup N such that*

$$\langle g \mid \mathrm{ind}(g) = \min_{g \neq e} \mathrm{ind}(g) \rangle \subset N, \tag{1.5}$$

(see definition of ind$(\cdot)$ *in Definition 2.2). More generally, given an counting invariant f (see Definition 2.1), we say G* is concentrated in N with respect to f *if $\langle g \mid f(g) = \min_{g \neq e} f(g) \rangle \subset N$.*

If G is concentrated with respect to discriminant or some other invariants, then the number of G-extensions with a fixed G/N-quotient is expected to be positive density among all G-extensions. In fact, this is exactly why the method in Alberts-Lemke-Oliver-Wang-Wood [AOWW24] is so effective in proving many more cases of Malle's conjecture when G is concentrated. We term this phenomena on the field counting side by

Definition 1.5 (Big Fiber)**.** *Let $\mathcal{F}(G^{inv}, X)$ be the number of G-extensions K with $inv(K) \leq X$. We say a field counting question G^{inv} over base field Q has a* big fiber over M *if there exists a nontrivial field extension $M \neq Q$ such that*

$$\liminf_{X\to\infty} \frac{\sharp\{K \in \mathcal{F}(G^{inv}, X) \mid M \subset \tilde{K}\}}{\sharp\{K \in \mathcal{F}(G^{inv}, X)\}} > 0. \tag{1.6}$$

It is very tempting to imagine that G being concentrated is equivalent to the existence of big fiber(s) in counting G-extensions (with respect to any invariant), or even stronger, that G being non-concentrated is equivalent to guarantee a good constant like an Euler product, which suggests good independence among different p. Unfortunately, both hopes are not true. In fact, even for $G = S_3$, the field counting question S_3^{rad} with product of ramified primes is already proven by [ST24] to have one big fiber over $\mathbb{Q}(\mu_3)$, even though S_3 is not concentrated with respect to product of ramified primes, not to mention the constant being one Euler product!

It is exactly for the same reason for Klüners to get his counter examples and for S_3^{rad} to have one big fiber. It is then very natural to push this reasoning further to get counterexamples for Conjecture 5 for general non-concentrated invariants.

Denoting $b_M(G^{\mathrm{rad}}, k)$ to be the b-constant appearing in Conjecture 5, we show that actually the original counter example of Klüners are already counterexamples for Conjecture 5.

Theorem 1.6. *Let ℓ be an odd prime and $G = C_\ell \wr C_{\ell-1}$. When $\ell \geq 5$, we have*

$$b(G^{rad}, \mathbb{Q}) > b_M(G^{rad}, \mathbb{Q}).$$

In fact, the lower bound is exactly established from counting G-extensions containing the $\mathbb{Q}(\mu_\ell)$. We also show the same phenomena to hold for other groups $G = C_\ell \wr C_m$ with $m|\ell - 1$ among Klüners' counterexamples, see Lemma 3.3.

We make a couple comments on these examples. Firstly, though it seems surprisingly simple, somehow it has been ignored by experts, see [KP23] where it is mistakenly commented that Klüners' counterexamples are not counterexamples for Conjecture 5 to support further pursuit of complicated ones. Secondly, as it can be seen, such a problem does not require subtle constraints on the underlying group structure of G. To indicate this in contrast to nilpotent examples in [KP23], we also give a convenient infinite family of nilpotent examples.

Theorem 1.7. *Let ℓ be an odd prime and $G = C_{\ell^2} \wr C_\ell$. When $\ell \geq 3$, we have*

$$b(G^{rad}, \mathbb{Q}) > b_M(G^{rad}, \mathbb{Q}). \tag{1.7}$$

Thirdly, even though in Lemma 3.3 we give the lower bound for $b(G^{\mathrm{rad}}, \mathbb{Q})$ from $b_\phi(G^{\mathrm{rad}}, C_\ell^d, \mathbb{Q})$, we don't expect them to be the true b in general. Finally these examples show that there doesn't seem to exist a unifying invariants, discriminant or product of ramified primes, that solves all the trouble once and for all.

1.4 A New Proposal

Now in retrospect of both types of examples represented, the intermediate subfield containing/not containing roots of unity can affect b constants easily from different mechanisms. We don't try to design any invariant to suppress the influence from roots of unity. The solution we propose in the following is a refined version of Malle's conjecture with general invariants following the exact spirit from global function fields, where G-extensions with particular fixed constant extensions are naturally grouped together. Here we split up $N_Q(G^{\mathrm{inv}}, X)$ to a finite set of subquestions according to the intersection of G-extensions with relevant cyclotomic extensions:

Conjecture 6 (Refined Malle's Conjecture)**.** *Let $G \subset S_n$ be a finite group, Q a global field with $(|G|, ch(Q)) = 1$. Let $d = lcm_{\exp(g)=\exp(G)} \mathrm{ord}(g)$. For any cyclotomic subfield $F \subset Q(\mu_d)$ with $\mathrm{Gal}(F/k) = B$ and a surjection $\pi : G \to B$, we define $N_{Q,\pi,\phi}(G^{inv}, X)$ to be the number of continuous surjective liftings $\tilde{\phi}$ such that:*

- *it makes the diagram commute:*

$$\begin{array}{ccccccccc} & & & & & & G_Q & & \\ & & & & & \swarrow^{\tilde{\phi}} & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & \mathrm{Ker}(\pi) & \longrightarrow & G & \xrightarrow{\pi} & B & \longrightarrow & 0 \end{array}$$

- *the fixed field $K_{\tilde{\phi}}$ associated to $\tilde{\phi}$ satisfying $K_{\tilde{\phi}} \cap k(\mu_d) = F$*
- *$inv(K_{\tilde{\phi}}) \leq X$*

We conjecture that either the above embedding problem is not solvable and $N_{Q,\pi,\phi}(G^{inv}, X) = 0$ or

$$N_{Q,\pi,\phi}(G^{inv}, X) = \Theta(X^{1/a(\pi,\phi)} \ln^{b(\pi,\phi)-1} X), \tag{1.8}$$

(when Q is the number field, replace Θ with $\sim$) where

$$a(\pi,\phi) := \min\{exp(g) \mid g \in \mathrm{Ker}(\pi)\}, \qquad b(\pi,\phi) := |\mathcal{C}_{min}(N^{inv})/G_Q| = b_\phi(G^{inv}, \mathrm{Ker}(\pi), Q), \tag{1.9}$$

where $\mathcal{C}_{min}(N^{inv})$ is the set of conjugacy classes of $\mathrm{Ker}(\pi)$ with $exp(g) = a(\pi,\phi)$ and G_Q acts on it via the ϕ-twisted action, i.e. $\sigma(\mathcal{C}_g) = \sigma \cdot \mathcal{C}_g^{\chi_{cyc}(\sigma)} \cdot \sigma^{-1}$.

It then follows as a consequence of Conjecture 6, that

Conjecture 7. *Given a transitive permutation group $G \subset S_n$ and a number field k. Denote $d = lcm_{g,\mathrm{ind}(g)=\mathrm{ind}(G)} \mathrm{ord}(g)$. We conjecture that*

$$b(G,k) = \max_{\mathrm{ind}(N)=\mathrm{ind}(G)} \max_{\phi} b_\phi(G, \mathrm{Ker}(\phi) = N, k), \tag{1.10}$$

where ϕ ranges over the finitely many continuous surjective maps $\phi : G_k \to G/N$ such that: 1) ϕ exactly cut out a cyclotomic subfield $F \subset k(\mu_d)$; 2) ϕ can be lifted to $\tilde{\phi}$ in 6

Comparing with Theorem 2.12, we now have the one more condition about the lifting property of ϕ. It is not entirely clear that we have realized all issues for understanding the b-constants. At the very least, we formulate Conjecture 6 to emphasize the importance of the counting function

$N_{Q,\pi,\phi}(G^{\text{inv}}, X)$, which is the exact analogue of Türkelli's context in global function fields and hasn't been translated to number fields in this way in the past.

Finally, we give the organization of this paper. In Section 2, we discuss predictions of $b(G, Q)$ in all situations. In particular, we give a simplified definition of $b_T(G, Q)$ in Theorem 2.12. In Section 3, we verify $b(G, Q)$ in all examples we listed in Theorem 1.3, Theorem 1.6 and Theorem 1.7. This includes computing the predictions from the group theoretic side and carrying over inductive argument to prove the true b. In Section 4, we discuss the difference of Problem 1.2 over function fields and number fields, and give the explicit criteria when G is solvable and G is abelian respectively.

2 Description of $b(G, k)$

In this section, we give a precise description of Malle's prediction $b_M(G, k)$ and Türkelli's modifiction $b_T(G, k)$. Although the original conjecture of Malle and Türkelli are both made only discriminant, for efficiency in discussing all theorems together, we define them with respect to general invariants once for all.

Following the spirit in [Woo10, Section 2.1], we give the following definition:

Definition 2.1 (Counting Invariant)**.** *Let $G \subset S_n$ be a finite permutation group and $\mathcal{C}(G)$ be the set of conjugacy classes of G. Let Q be a global field. Let $\exp : \mathcal{C}(G)\backslash\{e\} \to \mathbb{Z}_{>0}$ be a function where $\exp(g) = \exp(g^k)$ for any k that is relatively prime to $\text{ord}(g)$. For each place $v||G| \cdot \infty$, we define $\exp_v : \Sigma_v \to \mathbb{Z}_{\geq 0}$ where Σ_v is the set of continuous group homomorphisms $\rho_v : G_{Q_v} \to G \subset S_n$ (up to conjugation in S_n). Then for each G-extension K/Q with $\text{Gal}(K/Q) \simeq G \subset S_n$, equivalently given by a continuous surjective group homomorphism $\rho_K : G_Q \to G$, we define the* counting invariant *for K associated to f and f_v to be an integer denoted by $inv(K)$:*

$$inv(K) = \prod_{v||G|} |v|^{\exp_v(\rho_v)} \prod_{v|\infty} \exp_v(\rho_v) \prod_{v\nmid|G|} |v|^{\exp(y_v)}, \tag{2.1}$$

where y_v is any tame inertia generator at v in $\text{Gal}(K/Q)$.

For a general invariant inv, we use G^{inv} to denote the counting question with inv and $N_k(G^{\text{inv}}, X)$ to denote the counting function. For example, G^{rad} denotes the counting question with radical of discriminant. When we do not specify the invariant, our counting invariant for $G \subset S_n$ is the usual discriminant.

2.1 Malle's constant $b_M(G, k)$

We first describe the $a(G)$ constant in Conjecture 1.

Definition 2.2 (Index)**.** *Given a transitive permutation group $G \subset S_n$, we define the* index *for $g \neq e \in G \subset S_n$ to be*

$$\text{ind}(g) := n - \sharp\{\textit{cycles of } g\}.$$

Since conjugation does not change the cycle type in S_n, it is well-defined that the conjugacy class $\mathcal{C}_g$ associated to g has

$$\text{ind}(\mathcal{C}_g) := \text{ind}(g).$$

Then index *of G is defined as*

$$\text{ind}(G) := \min_{g\neq e} \text{ind}(g).$$

The integer $a(G)$ is exactly $\mathrm{ind}(G)$. Notice that $\mathrm{ind}(\cdot)$ is exactly the function $\exp(\cdot)$ when the counting invariant inv is discrminant, we in general define

$$a(G^{\mathrm{inv}}) := \min_{g \neq e} \exp(g). \tag{2.2}$$

We denote $\mathcal{C}_{min}(G^{\mathrm{inv}})$ to be the set of conjugacy classes $\mathcal{C}$ of G with minimal $\exp(\mathcal{C})$. We now define the cyclotomic action from the absolute Galois group G_Q on G (the definition of the action does not require the set is $\mathcal{C}_{min}(G^{\mathrm{inv}})$)

Definition 2.3 (Cyclotomic Action)**.** *Given any field Q, the* cyclotomic character *is the canonical homomorphism*

$$\chi_{cyc} : \mathrm{Gal}(Q^{sep}/Q) \to \mathrm{Aut}(\mu_\infty) \subset \hat{\mathbb{Z}}^\times = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times.$$

We define the cyclotomic action *of G_Q on a finite group G as $\sigma(g) = g^{\chi_{cyc}(\sigma)}$.*

Notice that since G is finite, $g^{\chi_{cyc}(\sigma)}$ only depends on the image $\chi_{cyc}(\sigma)$ in $\mathbb{Z}/|G|\mathbb{Z}$. More concretely, denote $d = |G|$, it suffices to consider the image of G_Q into $(\mathbb{Z}/d\mathbb{Z})^\times$. If $\sigma \in G_Q$ maps $\sigma(\mu_d) = \mu_d^a$, then $\sigma(g) = g^a$. And one can check $\sigma(\mathcal{C}_g) = \mathcal{C}_{g^a}$ is well-defined. In fact if a certain group element $g \in G$ has order m, then the action of $\sigma \in \mathrm{Gal}(Q^{\mathrm{sep}}/Q)$ on $\mathcal{C}_g$ can be already computed as $\mathcal{C}(g^{\chi_{cyc}(\sigma)})$ via its image in $(\mathbb{Z}/m\mathbb{Z})^\times$ already.

Remark 2.4. *Notice that the action factors through $\mathrm{Gal}(Q(\mu_d)/Q)$ where $d = lcm_{g \in \mathcal{C}_{min}(G^{inv})} \mathrm{ord}(g)$. This means that the base field dependence in $b_M(G^{inv}, Q)$ only depends on $\mathrm{Gal}(Q(\mu_d)/Q) \subset (\mathbb{Z}/d\mathbb{Z})^\times$.*

We now define

$$b_M(G^{\mathrm{inv}}, Q) := |\mathcal{C}_{min}(G^{\mathrm{inv}})/\mathrm{Gal}(Q^{\mathrm{sep}}/Q)|, \tag{2.3}$$

under the cyclotomic action from $\mathrm{Gal}(Q^{\mathrm{sep}}/Q)$. Malle in [Mal04] conjectures that for number fields Q, we have $b_M(G, Q) = b(G, Q)$ where G stands for the natural discriminant as the counting invariant. We now demonstrate the computation via the following example. It is also stated in [Klü12].

Example 2.5 (Wreath Product)**.** *Let $G = T \wr B \subset S_{tb}$ be the wreath product as a permutation group, where $T \subset S_t$ and $B \subset S_b$. Since $\mathrm{ind}((t_1, \cdots, t_b) \rtimes b) \geq \mathrm{ind}((t_1, \cdots, t_b) \rtimes e)$, we see $\mathrm{ind}(G) = \mathrm{ind}((t, e, \cdots, e)) \rtimes e$ where $\mathrm{ind}(t) = \mathrm{ind}(T)$. It is now easy to see that the only elements with this index is exactly in such a form. Therefore $\mathrm{ind}(G) = \mathrm{ind}(T)$ and $\mathcal{C}_{min}(G)$ has a bijection with $\mathcal{C}_{min}(T)$. Moreover the action from $\mathrm{Gal}(Q^{sep}/Q)$ is identical. Thus $b_M(G, Q) = b_M(T, Q)$.*

Given the fact that the Galois group of a relative T-extension over a B-extension has Galois group embedded into $T \wr B$, this example immediately implies that Conjecture 1 cannot be true in general, since it is not consistent with itself since the total counting of all permutation Galois groups that arises as a relative T-extension over a B-extension can add up to be smaller than the number of relative T-extensions for a fixed cyclotomic B-extensions.

2.2 Türkelli's constant $b_T(G, k)$

In this section, we revisit Türkelli's modification on Malle's constant b in [Tür15]. This is of crucial importance, since it is often not being interpreted correctly. We also give a simplified form of it in Theorem 2.12.

Let G be a transitive permutation group and $N \subset G$ a normal subgroup and Q a global field. For each continuous group homomorphism $\phi : G_Q \to B := G/N$, we recall the ϕ-twisted cyclotomic action:

Definition 2.6 (ϕ-twisted cyclotomic action)**.** *Fix $N \subset G$ and $\phi : G_Q \to B = G/N$. For each conjugacy class $\mathcal{C}_n$ in N and $\sigma \in G_Q$, let $\bar{\sigma}$ be any lift of $\phi(\sigma) \in B$ in G. We define the ϕ-twisted cyclotomic action of G_Q on conjugacy classes of N as:*

$$\sigma(\mathcal{C}_n) = \bar{\sigma} \cdot {\mathcal{C}_n}^{\chi_{cyc}(\sigma)} \cdot \bar{\sigma}^{-1}.$$

The action on conjugacy classes does not depend on the choice of $\bar{\sigma}$.

Notice that unlike the cyclotomic action, such an action can only be defined on conjugacy classes of N instead of N, due to non-uniqueness of choice of $\bar{\sigma}$. This action is only defined in [Tür15] for abelian and cyclotomic ϕ, i.e., ϕ factor through $G_{Q^{cyc}} \to B$ where Q^{cyc} is the cyclotomic closure of Q.

Now fix a counting invariant inv for $G \subset S_n$ and let $\exp(G) := \min_{g \neq e} \exp(g)$. We can naturally extend exp to any normal subgroup $N \subset G$, and define $\exp(N) := \min_{n \neq e} \exp(n)$, and

$$\mathcal{C}_{min}(N^{\mathrm{inv}}) := \{\text{conjugacy class } \mathcal{C} \subset N (\text{conjugation in } N) \mid \exp(\mathcal{C}) = \exp(N)\}.$$

Be careful that here we are taking conjugacy classes of N with the conjugation only coming from N but not G. We then define for each ϕ that

$$b_\phi(G^{\mathrm{inv}}, N, Q) := |\mathcal{C}_{min}(N^{\mathrm{inv}})/G_Q|. \tag{2.4}$$

Remark 2.7. *In [Tür15] this definition of b-constants is only stated for ϕ corresponding to abelian extensions. We follow [Alb22] to define it for general ϕ. In [Alb22] this particular $b_\phi(G, N)$ is conjectured to describe the asymptotic distribution for general N-torsors over a fixed ϕ. This is how we should think about it morally. It is justified with a heuristic argument similarly like how Malle's original conjecture is justified. It is also verified to be the correct b when N is abelian, parallel to that Malle's original conjecture also holds for all abelian extensions. However Klüners counterexample still stands as counterexamples for these more general conjectures.*

With this notation Türkelli defines that if $\mathrm{Sur}(G_{Q^{cyc}}, G/N)$ is non-empty then

$$b(G^{\mathrm{inv}}, N, Q) := \max_{\phi \in \mathrm{Sur}(G_{Q^{cyc}}, G/N)} b_\phi(G^{\mathrm{inv}}, N, Q), \tag{2.5}$$

and otherwise $b(G^{\mathrm{inv}}, N, Q) = 0$.

Definition 2.8 (Türkelli's Modified b)**.** *Given a global field Q and G^{inv},*

$$b_T(G^{inv}, Q) := \max_{N \lhd G, \exp(N) = \exp(G)} b(G^{inv}, N, Q). \tag{2.6}$$

For inv = disc, we have

$$b_T(G, Q) := \max_{N \lhd G, \mathrm{ind}(N) = \mathrm{ind}(G)} b(G, N, Q). \tag{2.7}$$

We remark that Türkelli [Tür15] only formulates his conjecture for discriminant. We take the liberty of calling it b_T for general invariants, with the same spirit carried over.

We make two comments. Firstly, it is clear that $b(G^{\mathrm{inv}}, G, Q) = b_M(G^{\mathrm{inv}}, Q)$ when $N = G$, therefore

Lemma 2.9. *Given $G \subset S_n$ and global field Q, it always holds that*

$$b_M(G,Q) \leq b_T(G,Q). \tag{2.8}$$

This also holds for general counting invariant inv.

Secondly, over function field Q^{cyc} is simply $Q \cdot \bar{F}_p$ which is cyclic, however over number fields Q^{cyc} is not, in fact it is countably many generated over any number field. This means that determining $b_T(G,Q)$ involves checking for infinite many ϕ for number fields but finitely many for function fields. Therefore we make the following simplification for number field.

We first give an alternative definition for $b_\phi(G^{\text{inv}}, N, Q)$. Given $\phi : G_Q \to G/N$ surjective, denote $Q(\phi)/Q$ to be the corresponding G/N-extension. Let $d := \text{lcm}_{n \in \mathcal{C}_{min}(N^{\text{inv}})} \text{ord}(n)$. We now define the finite group

$$\tilde{G} := G \times_{\text{Gal}(Q(\phi) \cap Q(\mu_d)/Q)} \text{Gal}(Q(\mu_d)/Q))$$

where the fibering map is defined to be the natural quotient. Under the fiber product notation, $(x,y) \in G$ iff $\bar{x} = \bar{y} \in \text{Gal}(Q(\phi) \cap Q(\mu_d)/Q)$. We now define the action of $\tilde{G}$ on $\mathcal{S}_{min}(N^{\text{inv}}) := \{n \in N \mid \exp(n) = \exp(N)\}$:

$$(x,y) \cdot n = x \cdot n^{\chi_{cyc}(y)} \cdot x^{-1}.$$

Notice that $\mathcal{S}_{min}(N^{\text{inv}})/(N \times e \subset \tilde{G}) = \mathcal{C}_{min}(N^{\text{inv}})$, and for any group action $X/G = (X/N)/(G/N)$, we thus obtain:

Lemma 2.10. *Given $N \subset G \subset S_n$, $\phi : G_Q \to G/N$ where Q is any global field, and any counting invariant inv,*

$$b_\phi(G^{inv}, N, Q) = |\mathcal{S}_{min}(N^{inv})/\tilde{G}|. \tag{2.9}$$

Now we can compare $b_\phi(G^{\text{inv}}, N, Q)$ among different ϕ, even different N.

Lemma 2.11. *Given $G \subset S_n$, Q any global field, and any counting invariant inv. Let N_i, $i = 1,2$ be two normal subgroups of G with $\exp(N_i) = \exp(G)$.*
1) If $X := \{g \in G \mid \exp(g) = \exp(G)\} \cap N_1 = \{g \in G \mid \exp(g) = \exp(G)\} \cap N_2 \neq \emptyset$. Let $d = lcm_{n \in X} \text{ord}(n)$. Given two surjections $\phi_i : G_Q \to G/N_i$. If the corresponding G/N_i-extension $Q(\phi_i)$ has $(Q(\phi_1) \cap Q(\mu_d)) \subset (Q(\phi_2) \cap Q(\mu_d))$, then

$$b_{\phi_1}(G^{inv}, N_1, Q) \leq b_{\phi_2}(G^{inv}, N_2, Q), \tag{2.10}$$

with the equality happens if the field inclusion is equality.
2) If $N_1 \subset N_2$, let $d = lcm\{\text{ord}(g) \mid \exp(g) = \exp(G)\}$. If the surjective homomorphisms $\phi_i : G_Q \to G/N_i$ satisfy that $Q(\phi_1) \cap Q(\mu_d) = Q(\phi_2)$, then

$$b_{\phi_1}(G^{inv}, N_1, Q) \leq b_{\phi_2}(G^{inv}, N_2, Q). \tag{2.11}$$

with the equality happens if $\{g \in G \mid \exp(g) = \exp(G)\} \cap N_1 = \{g \in G \mid \exp(g) = \exp(G)\} \cap N_2$.

Proof. With $(Q(\phi_1) \cap Q(\mu_d)) \subset (Q(\phi_2) \cap Q(\mu_d))$, we obtain a natural embedding $\tilde{G}_2 \to \tilde{G}_1$: using the fiber product notation, $(x,y) \in \tilde{G}_2$ with $\bar{x} = \bar{y} \in \text{Gal}(Q(\phi_2) \cap Q(\mu_d))$ always satisfy $\bar{x} = \bar{y} \in \text{Gal}(Q(\phi_1) \cap Q(\mu_d))$. The action of (x,y) remains the same and the set X being acted is the same. Therefore the number of orbits with $\tilde{G}_2$ is greater or equal. Therefore we prove the first statement. Reversing ϕ_1 and ϕ_2 implies we obtain equality when the field inclusion is equality.

For the second statement, It is clear from the above argument that $\tilde{G}_1 = \tilde{G}_2$, and the minimal exponent element is clearly a bigger set for N_2. □

We observe now from the first statement, when $N_1 = N_2 = N$, Lemma 2.11 implies that it suffices to take ϕ with $Q(\phi)$ with maximal $Q(\phi) \cap Q(\mu_d) \subset Q(\mu_d)/Q$ for any fixed N. Then it follows from the second statment, if the maximal $Q(\phi)$ (not necessarily unique) from last step satisfies $Q(\phi) \cap Q(\mu_d) \neq Q(\phi)$, it also suffices to check the natural quotient $\bar{\phi}$ where $Q(\bar{\phi})$ corresponds to the $Q(\phi) \cap Q(\mu_d)$.

Theorem 2.12. *Given $G \subset S_n$, Q a global field, and $d = lcm\{\mathrm{ord}(g) \mid \exp(g) = \exp(G)\}$. We have the following equality:*

$$b_T(G^{inv}, Q) = \max_{N, \exp(N)=\exp(G)} \max_{\phi} b_\phi(G^{inv}, N, Q), \tag{2.12}$$

where the maximum is taken among $\phi : G_Q \to G/N$ that is surjective and factors through $\mathrm{Gal}(Q(\mu_d)/Q)$, that is, exactly cut out subfield of $Q(\mu_d)/Q$.

Notice that given $Q(\mu_d)/Q$ being finite, it is now a finite checking with ϕ exactly corresponding to subfields of $Q(\mu_d)$.

3 Computation of $b(G, Q)$

In this section, we verify various b-constants in Conjecture 1, Conjecture 3, Conjecture 5 and the true value.

3.1 Group Constant Computation

In this section, we give the group theoretic computation of predictions for b-constants from Malle and Türkelli.

We first give the computation towards showing Theorem 1.3.

Lemma 3.1. *Let ℓ be an odd prime number and $d = \prod_i p_i^{r_i}$ where p_i are all prime numbers. Let $G = C_\ell \wr C_d \subset S_{\ell d}$ and $\gcd(q, |G|) = 1$. If $\gcd(d, \ell - 1) = \prod_i p_i^{s_i}$ then*

$$b_T(G, \mathbb{Q}) = \gcd(d, \ell - 1) \qquad b_M(G, \mathbb{Q}) = 1.$$

Proof. By Example 2.5, we have $b_M(G, \mathbb{Q}) = b_M(C_\ell, \mathbb{Q}) = 1$. We now compute $b_T(G, \mathbb{Q})$. Firstly, we only need to consider those $N \supset C_\ell^d$, since C_ℓ^d is normally generated by any minimal index element. By Theorem 2.12 and Lemma 2.11, it suffices to consider $\phi : G_{\mathbb{Q}} \to \mathbb{Z}/\gcd(d, \ell - 1)\mathbb{Z}$ correspond to the unique subfield of $\mathbb{Q}(\mu_\ell)$ with degree $\gcd(d, \ell - 1)$. We now compute $b_\phi(G, N, \mathbb{Q})$. It is easy to count that $|\mathcal{C}_{min}(N)| = (\ell - 1)\gcd(d, \ell - 1)$. The action from $G_{\mathbb{Q}}$ factors through $\mathbb{Z}/\gcd\mathbb{Z}$, therefore it is enough to consider the action from the generator of $\mathbb{Z}/\gcd\mathbb{Z}$. The orbit length for each class is exactly $\ell - 1$, therefore the number of orbits is exactly $\gcd(d, \ell - 1)$. □

Remark 3.2. *We remark that by a simple group theoretic consideration: in Lemma 3.3*

$$b_\phi(C_\ell^{\ell-1}, C_\ell \wr C_{\ell-1}) = b_M(C_\ell, F_\phi), \tag{3.1}$$

and in Lemma 3.4,

$$b_\phi(C_{C_\ell}^{\ell^2}, G^{rad}, \mathbb{Q}) = b_M(C_{\ell^2}^{rad}, F_\phi). \tag{3.2}$$

We next give the computation towards showing Theorem 1.6

Lemma 3.3. *Let ℓ be an odd prime and $m|\ell-1$ with $m>2$, $G=C_\ell \wr C_m$ and $N=C_\ell^m$. Let ϕ corresponds to the unique C_m subfield contained in $\mathbb{Q}(\mu_\ell)$. We then have*

$$b_\phi(G^{rad},N,\mathbb{Q}) \gg b_M(G^{rad},\mathbb{Q}). \tag{3.3}$$

For $m=\ell-1$ and $\ell\geq 5$,

$$b_\phi(G^{rad},N,\mathbb{Q}) > b_M(G^{rad},\mathbb{Q}). \tag{3.4}$$

Proof. The conjugacy classes of $C_\ell \wr C_{\ell-1}$ come in two types: contained in N and outside of N. Within N, the class represented by $(a_1,\cdots,a_{\ell-1})\rtimes e$ contains all rotations of a_i, i.e. , $(a_i,a_{i+1},\cdots,a_{\ell-1},a_1,\cdots,a_{i-1})\rtimes e$ for certain i. Outside N, we have $(a_1,\cdots,a_{\ell-1})\rtimes\sigma$ conjugate to $(b_1,\cdots,b_{\ell-1})\rtimes\tau$ if and only if $\tau=\sigma$ and $\sum_i a_i=\sum_i b_i$.

We first compute $b_M(G^{\mathrm{rad}},\mathbb{Q})$. We first count the number of $G_\mathbb{Q}$-orbits within N. Notice that the conjugation of G on N purely comes from $G/N=C_{\ell-1}$ and all nontrivial elements in N have order ℓ, it then suffices to count the orbits for $G/N\times\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ acting on $X=N\backslash\{e\}$ where $(x,y)\cdot n=x\cdot n^{\chi_{cyc}(y)}\cdot x^{-1}$. By Burnside's Lemma, the number of orbits is

$$|X/(G/N\times\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}))| = \frac{1}{|C_{\ell-1}\times C_\ell^\times|}\sum_{g\in C_{\ell-1}\times C_\ell^\times}|X^g|, \tag{3.5}$$

Let $g=(r,s)$, then X^g corresponds to the non-trivial eigenvectors of r with eigenvalue s. If r generates $C_{\ell-1}$, then as a linear operator r satisfies $r^{\ell-1}-1=\prod_{\lambda\in\mathbb{F}_\ell^\times}(r-\lambda)=0$, which shows that every scalar is an eigenvalue and each eigenvalue has 1-dim eigenspace. Thus we compute that $|X^g|$ for (r,s) is $\ell-1$ for this case. Similarly, when r has order smaller than $\ell-1$, the operator r has $(\ell-1)/\operatorname{ord}(r)$ identical invariant spaces with dimension $\operatorname{ord}(r)$, within which all $\operatorname{ord}(r)$-th roots of unity in $\mathbb{F}_\ell^\times$ are eigenvalues with 1-dim eigenspace. Therefore if $s^{\operatorname{ord}(r)}=1$, we obtain $|X^g|=\ell^{(\ell-1)/\operatorname{ord}(r)}-1$. Now we compute the number of orbits within N is

$$\frac{1}{(\ell-1)^2}\sum_{r\in C_{\ell-1}}\operatorname{ord}(r)\cdot\left(\ell^{(\ell-1)/\operatorname{ord}(r)}-1\right)\leq\frac{1}{(\ell-1)^2}\Big(\ell^{\ell-1}-1+(\ell-2)(\ell-1)\cdot\ell^{(\ell-1)/2}\Big), \tag{3.6}$$

with the leading term comes from $g=e$. Notice the total number of classes outside N is $(\ell-2)\cdot\ell$, we then have

$$b_M(G^{\mathrm{rad}},\mathbb{Q})\leq\frac{1}{(\ell-1)^2}\Big(\ell^{\ell-1}-1\Big)+\frac{\ell-2}{\ell-1}\cdot\ell^{(\ell-1)/2}+(\ell-2)\cdot\ell. \tag{3.7}$$

Now we compute $b_\phi(G^{\mathrm{rad}},N,\mathbb{Q})$ where $\phi:G_\mathbb{Q}\to C_{\ell-1}$ corresponds to $\mathbb{Q}(\mu_\ell)/\mathbb{Q}$. By Lemma 2.10, it suffices to consider $\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ acts on $X=N\backslash\{e\}$ via the ϕ-twisted action, i.e., $x\cdot n=x\cdot n^{\chi_{cyc}(x)}\cdot x^{-1}$. By Burnside's Lemma, the number of orbits is only the sum over (r,r) in previous computation:

$$b_\phi(G^{\mathrm{rad}},N,\mathbb{Q})=\frac{1}{\ell-1}\sum_{r\in C_{\ell-1}}\left(\ell^{(\ell-1)/\operatorname{ord}(r)}-1\right)\geq\frac{|X^e|+(\ell-2)(\ell-1)}{\ell-1}=\frac{\ell^{\ell-1}-1}{\ell-1}+(\ell-2). \tag{3.8}$$

It is checked that when ℓ is large enough (i.e. $\ell\geq 5$) we have

$$b_\phi(N,G^{\mathrm{rad}},\mathbb{Q})>b_M(G^{\mathrm{rad}},\mathbb{Q}).$$

For $m|\ell-1$ and $G=C_\ell\wr C_m$, we can similarly compute $b_M(G,\mathbb{Q})$ and $b_\phi(G,N,\mathbb{Q})$ where $\phi:G_\mathbb{Q}\to C_m$ corresponds to the unique C_m quotient of $\mathbb{Q}(\mu_\ell)$. The number of conjugacy classes

outside N is $(m-1)\cdot\ell$. For elements inside N, we consider $C_m \times \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ acting on $X = N\backslash e$ to determine its contribution to $b_M(G,\mathbb{Q})$. Thus by Burnside's Lemma, we have

$$b_M(G,\mathbb{Q}) \leq (m-1)\cdot\ell + \frac{1}{(\ell-1)m}\sum_{r\in C_m} \mathrm{ord}(r)\cdot(\ell^{m/\mathrm{ord}(r)}-1) \leq \frac{\ell^m-1}{(\ell-1)m} + \frac{m-1}{\ell-1}\cdot\ell^{m/2} + (m-1)\cdot\ell. \tag{3.9}$$

To compute $b_\phi(G,N,\mathbb{Q})$, it suffices to consider $\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ acting on the same set X with the same action that $x\cdot n = x\cdot n^{\chi_{cyc}(x)}\cdot x^{-1}$. The orbit number is at least

$$b_\phi(G,N,\mathbb{Q}) = \frac{1}{\ell-1}\sum_{r\in C_m}\left(\ell^{m/\mathrm{ord}(r)}-1\right) \geq \frac{\ell^m-1}{\ell-1} + \frac{m-1}{\ell-1}\cdot(\ell-1) = \frac{\ell^m-1}{\ell-1} + (m-1). \tag{3.10}$$

Therefore for $m>2$, we have $b_\phi(G,N,\mathbb{Q}) \gg b_M(G,\mathbb{Q})$. □

We finally give the computation towards showing Theorem 1.7.

Lemma 3.4. *Let ℓ be an odd prime, $G = C_{\ell^2} \wr C_\ell$ and $N = C_\ell^\ell$. For $\ell \geq 3$, and ϕ corresponds to the unique C_ℓ-extension only ramified at ℓ over $\mathbb{Q}$, we have*

$$b_\phi(N, G^{rad}, \mathbb{Q}) > b_M(G^{rad}, \mathbb{Q}).$$

Proof. Similarly with Lemma 3.3, there are two types of conjugacy classes of $C_{\ell^2} \wr C_\ell$. The description of these classes also follow exactly the same rule. We focus on those contained in N, since the number of conjugacy classes outside N is bounded from above by $(\ell-1)\ell^2$.

We first compute $b_M(G^{\mathrm{rad}},\mathbb{Q})$. The cyclotomic action from $G_\mathbb{Q}$ on conjugacy classes within N is from $\mathrm{Gal}(\mathbb{Q}(\mu^2)/\mathbb{Q})$. We apply Burnside's Lemma where $X = C_{\ell^2}^\ell\backslash\{e\}$ acted by $C_\ell \times \mathrm{Gal}(\mathbb{Q}(\mu^2)/\mathbb{Q})$. The action from C_ℓ is rotation and the action from $\mathrm{Gal}(\mathbb{Q}(\mu^2)/\mathbb{Q}) \simeq \mathbb{C}_{\ell^2}^\times$ is scalar multiplication. We have $|X^e| = \ell^{2\ell}-1$. If $r=0$ then for $g=(r,s)$ we have $|X^g| = \ell^\ell - 1$ if $s \equiv 1 \mod \ell$ and $|X^g| = 0$ if not. If $r\neq 0$ generates C_ℓ and $s=1$, then X^g are all the constant vectors, therefore $|X^g| = \ell^2-1$. If $r\neq 0$ and $s\neq 0$, then X^g contains scalar multiplications of $(1,s,\cdots,s^{\ell-1})$ if $s^\ell = 1$ (i.e., $s\equiv 1 \mod \ell$) and X^g is empty if $s^\ell \neq 1$. Therefore summing up all terms, we obtain that the number of orbits within N is

$$\frac{1}{\ell^2(\ell-1)}\Big(\ell^{2\ell} - 1 + \ell\cdot(\ell^\ell-1) + (\ell-1)\cdot\ell\cdot(\ell^2-1)\Big). \tag{3.11}$$

Now we compute $b_\phi(N, G^{\mathrm{rad}}, \mathbb{Q})$ where $\phi: G_\mathbb{Q} \to C_\ell$ be corresponding to the unique degree ℓ sub-extension $F/\mathbb{Q}$ in $\mathbb{Q}(\mu^2)/\mathbb{Q}$. To count the number of orbits with Burnside's Lemma, we have $X = N\backslash\{e\}$ acted by $\mathrm{Gal}(\mathbb{Q}(\mu^2)/\mathbb{Q})$. Notice that the number of orbits is at least

$$\frac{|X^e|}{\ell(\ell-1)} = \frac{\ell^{2\ell}-1}{\ell-1}. \tag{3.12}$$

When $\ell \geq 3$, we have

$$b_\phi(N, G^{\mathrm{rad}}, \mathbb{Q}) > b_M(G^{\mathrm{rad}}, \mathbb{Q}).$$

□

3.2 Field Counting: Number Fields

In this subsection, we give statements on $b(G,\mathbb{Q})$ and $b(G^{rad},\mathbb{Q})$ in Theorem 1.3, Theorem 1.6 and Theorem 1.7.

Lemma 3.5. *Let ℓ be an odd prime number and $d = \prod_i p_i^{r_i} \neq 2$ where p_i are all prime numbers. Let $G = C_\ell \wr C_d \subset S_{\ell d}$ and $\gcd(q, |G|) = 1$. Denote $\gcd(d, \ell - 1) = \prod_i p_i^{s_i}$. Let $s = val_2(\ell - 1) - 1$ when $val_2(d) > val_2(\ell - 1)$ and $s = 0$ otherwise. Then*

$$b(G, \mathbb{Q}) = \prod_{i, r_i = s_i} p_i^{s_i} \cdot 2^s.$$

Proof of Theorem 1.3, over $\mathbb{Q}$. By [AOWW24, Corollary 1.6] for $d > 2$ and $G = C_\ell \wr C_d$ the inequality is satisfied as

$$\frac{1}{2} + \frac{p}{d(p-1)} < \frac{\ell}{\ell - 1},$$

where p is the minimal prime divisor of d. Then we have

$$b(G, \mathbb{Q}) = \max_{F/\mathbb{Q}, \mathrm{Gal}(F/\mathbb{Q}) = C_d} b(C_\ell, F). \tag{3.13}$$

For $G = C_\ell$, by [Wri89], $b(F, C_\ell) = b_M(F, C_\ell) = [F \cap \mathbb{Q}(\mu_\ell) : \mathbb{Q}]$.

Recall the notation $\gcd(d, \ell - 1) = \prod_i p_i^{s_i}$ and $d = \prod_i p_i^{r_i} \neq 2$, and denote $\ell - 1 = \prod_i p_i^{u_i}$, that is, $s_i = \min\{r_i, u_i\}$. Since $\mathbb{Q}(\mu_\ell)$ is cyclic over $\mathbb{Q}$, for each $n | \gcd(d, \ell - 1)$, there exists a unique cyclotomic subfield $M = M_n \subset \mathbb{Q}(\mu_\ell)$ that is only ramified at ℓ with degree n over $\mathbb{Q}$. Given $n = \prod_i p_i^{t_i}$ with $0 \leq t_i \leq s_i$, it follows from Theorem 4.2 that M_n can be embedded into a C_d-extension if and only if 1) $\ell \equiv 1 \mod p_i^{r_i}$ for each $p_i | n$, and 2) if M_n is totally imaginary, then $\mathrm{val}_2(d) = \mathrm{val}_2(n)$. Notice that $\ell \equiv 1 \mod p_i^{u_i}$, the first condition amounts to saying that $u_i \geq r_i$ whenever $t_i > 0$, equivalently, $s_i = r_i$. For the second condition, M_n is totally imaginary iff $n \nmid (\ell - 1)/2$ iff $\mathrm{val}_2(n) = \mathrm{val}_2(\ell - 1)$. Thus in this case, we require $\mathrm{val}_2(d) = \mathrm{val}_2(n) = \mathrm{val}_2(\ell - 1)$, i.e., $r_i = t_i = u_i$. Therefore the maximal n where M_n can be embedded into a C_d-extension can be described by specifying t_i: at odd primes, if $u_i \geq r_i$ (i.e., $r_i = s_i$), then let $t_i = s_i = r_i$, otherwise 0; at $p = 2$, if $r_i = u_i$, then we let $t_i = r_i = u_i = s_i$, if $r_i < u_i$, then we let $t_i = s_i = r_i$, if $r_i > u_i$, then we let $t_i = s_i - 1 = u_i - 1$. It then follows that $b(T, \mathbb{Q})$ is this particular n, which is $\prod_{r_i = s_i} p_i^{s_i} \cdot 2^s$ where $s = \mathrm{val}_2(\ell - 1) - 1$ only when $\mathrm{val}_2(d) > \mathrm{val}_2(\ell - 1)$. □

Next we compute a lower bound for $b(G^{\mathrm{rad}}, \mathbb{Q})$ for $G = C_\ell \wr C_d$ and $C_{\ell^2} \wr C_\ell$.

Lemma 3.6. *For $G = C_\ell \wr C_d \subset S_{\ell d}$ with respect to $N = C_\ell^d$ and $G = C_{\ell^2} \wr C_\ell \subset S_{\ell^3}$ with respect to $N = C_{\ell^2}^\ell$. We show that*

$$b(G^{rad}, \mathbb{Q}) \geq b_\phi(G^{rad}, N, \mathbb{Q}).$$

Proof. By taking $T = N$, this can be translated to [AO21, Alb22] and choosing any $\pi : G_\mathbb{Q} \to G$ such that its natural restriction $\pi : G_\mathbb{Q} \to G/N$ corresponds to the cyclotomic extension $F = \mathbb{Q}(\mu_\ell)$ (respectively the unique C_ℓ-subfield F contained in $\mathbb{Q}(\mu_{\ell^2})$). Since they are wreath product, there exists G extensions containing F. We then obtain that the number of G-extension containing F with $\mathrm{rad} < X$ has an asymptotic distribution with $a(G^{\mathrm{inv}}) = 1$ and $b_\phi(G^{rad}, N, \mathbb{Q})$. This gives a lower bound on $b(G^{\mathrm{rad}, \mathbb{Q}})$ already. □

3.3 Field Counting: Global Function Fields

Our main task in this section is to give a proof for the following lemma to prove Theorem 1.3:

Lemma 3.7. *Let ℓ be an odd prime number and $d = \prod_i p_i^{r_i} \neq 2$ where p_i are all prime numbers. Let $G = C_\ell \wr C_d \subset S_{\ell d}$ and $\gcd(q, |G|) = 1$, $\mathrm{Gal}(\mathbb{F}_q(t)(\mu_\ell)/\mathbb{F}_q(t)) = \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. Denote $\gcd(d, \ell - 1) = \prod_i p_i^{s_i}$.*

$$b(G, \mathbb{F}_q(t)) = b_T(G, \mathbb{F}_q(t)) = \prod_i p_i^{s_i}.$$

Analogous with the number field setting, for each X, we denote $N_{\mathbb{F}_q(t)}(G,X)$ to be the number of all G-extensions over $\mathbb{F}_q(t)$ with discriminant bounded by X. For us, in order to complete parallel statements with number fields, the discriminant of a G-extension $K/\mathbb{F}_q(t)$ is the product of local discriminant over all primes away from the chosen infinity place.

We point out a couple differences for counting extensions over global function fields, from that over number fields. The **first** difference from Malle's conjecture over number field is that, we cannot state an asymptotic distribution for $N_{\mathbb{F}_q(t)}(G,q^m)$, since there might not exist extensions with discriminant exactly q^m. Combining the fact that all discriminant now is q^m, a precise asymptotic does not exist whenever we get the non-existence (e.g. $G=C_3$ over $\mathbb{F}_q(t)$), no matter if we choose to count extensions with discriminant bounded by q^m or exactly equal to q^m. Due to this reason, we state the corresponding Malle's conjecture over function fields in Conjecture 2 with $\Theta(\cdot)$ instead of $\sim$.

Before we start the proof, we first give the following reformulation of Wright's result [Wri89] for abelian extensions when the abelian group A has $(|A|,q)=1$. Notice that [Wri89, Theorem I.3] only states certain weighted partial sum for abelian extensions. We now show it implies Conjecture 2 for abelian group A.

Theorem 3.8. *Conjecture 2 holds for abelian group A when $(|A|,q)=1$.*

Proof. Let Q be a global function field and a_{q^m} denotes the number of A-extensions over k with discriminant exactly equal q^m. Recall that Wright has proved the statement that

$$\sum_{j=0}^{b-1} a_{q^{m+j}}\cdot q^{-j/a}\sim C(q^m)^{1/a}\cdot P_{b-1}(m)+O(q^m)^{1/a-\delta}, \tag{3.14}$$

where $a=a(A)$ and $b=b_M(A,Q)$, and P_{b-1} is a polynomial with degree $b-1$ and $\delta>0$ is a small positive number. Summing the equation from 1 to m and rearrange the terms, we obtain

$$N_Q(A,q^m)\cdot(\sum_j q^{-j/a})+\sum_{1\le j\le b-1}\sum_{1\le k\le j} a_{q^{m+k}}\cdot q^{-(b-j)/a}\sim C\sum_{1\le i\le m}(q^i)^{1/a}\cdot P_{b-1}(i)+O(q^m)^{1/a-\delta}. \tag{3.15}$$

Notice that the summation over i on the right hand side is also $q^{m/a}\cdot\tilde{P}_{b-1}(m)$ with $\tilde{P}$ a degree $b-1$ polynomial. It immediately follows that $N_Q(A,q^m)\le C_2q^{m/a}m^{b-1}$ for some C_2.

To see the lower bound, notice that

$$N_Q(A,q^m)\cdot(\sum_j q^{-j/a})\ge C\sum_{1\le i\le m-b+1}(q^i)^{1/a}\cdot P_{b-1}(i)+O(q^m)^{1/a-\delta}. \tag{3.16}$$

which implies that there exists C_1 such that

$$N_Q(A,q^m)\ge C_1q^{m/a}m^{b-1}. \tag{3.17}$$

□

To determine $b(G,\mathbb{F}_q(t))$ for $G=C_\ell\wr C_d\subset S_{\ell d}$, we follow the similar idea in [AOWW24]. The plan is to apply Theorem 3.8 to $G=C_\ell$ over any C_d-extension $F/\mathbb{F}_q(t)$. For each F and corresponding ϕ, by Remark 3.2, we have $b_\phi(C_\ell^d,C_\ell\wr C_d,k)=b_M(C_\ell,F)=b(C_\ell,F)$. Therefore it suffices to prove that: a)

$$b(G,\mathbb{F}_q(t))=\max_{F,\mathrm{Gal}(F/\mathbb{F}_q(t))=C_d} b(C_\ell,F), \tag{3.18}$$

and b)

$$\max_{F,\mathrm{Gal}(F/\mathbb{F}_q(t))=C_d} b(C_\ell, F) = \max_{\phi} b_\phi(C_\ell \wr C_d, C_\ell^d, \mathbb{F}_q(t)) = b_T(G, \mathbb{F}_q(t)), \tag{3.19}$$

where ϕ varies over all $G_{\mathbb{F}_q(t)} \to C_d$. In (3.19), the first equality is tautological, and the second equality follows from Theorem 4.1: indeed, all abelian quotient G/N with $\mathrm{ind}(N) = \mathrm{ind}(G)$ must contain $N = C_\ell^d$, and if $\bar{\phi}$ with smaller quotient can be lifted to ϕ with C_d-quotient, then by Lemma 2.11 case 1, it suffices to check all C_d-quotient. Theorem 4.1 and Theorem 4.2 forms the **second** major difference of function fields over number fields: not every cyclotomic extension can be embedded into a bigger cyclotomic extension over number field, but they always do over function field. See Section 4 for more discussion. This is the main reason leading to the difference of b-constants over function fields and number fields in this paper.

Finally, it remains to prove (3.18), that is, the analogue of the inductive argument in [AOWW24] over function field. We sketch the idea as following. For each C_d-extension, we need to count $N_F(C_\ell, X$ over a general C_d-extension $F/\mathbb{F}_q(t)$ with the predicted a and b-constants, in addition to an upper bound on $N_F(C_\ell, F)$ with a uniform dependence on $\mathrm{Disc}(F)$ that is small. Finally, adding up all $N_F(C_\ell, X)$ with the uniform dependence to show the total counting satisfy (3.18). We now point out a **third** interesting difference over function fields from number fields. The uniform dependence on counting abelian extensions are exactly characterized by the size of the ℓ-torsion in class groups of F, which can be bounded by $\mathrm{Disc}(F)^{1/2-\delta}$ with different δ depending on what $\mathrm{Gal}(F)$ is. See [AOWW24] for relevant references. The ℓ-torsion of the class group for a function field $F/\mathbb{F}_q(t)$, instead of being bounded by $\mathrm{Disc}(F)^\delta$ for some fixed $\delta > 0$, has a trivial bound ℓ^{2g} where g is the genus and is linearly determined by the discriminant of F via Riemann Hurwitz formula. When q becomes larger and larger, the trivial bound behaves better and better and can be considered as bounded by D^ϵ for arbitrary small ϵ, as long as q is taken to be large enough with respect to ϵ. This leads to many more cases of Malle's conjecture being proved over function field.

Before we give the proof, let's first give a summary of the class field theory over function fields. For us, given a finite function field $F/\mathbb{F}_q(t)$, we obtain the ring of integers O_F that contains all elements that are integral over all finite places (not including the places above ∞), which is the integral closure of $\mathbb{F}_q[t]$ inside F. We define the ideal class group of F to be the class group of the ring O_F. It is a classical theorem that the ideal class group is also finite for function fields. But unlike number fields, F can have many infinite unramified extension, which is just the constant finite field extension. Relating the ideal class group with idéle class group C_F, we obtain the following

$$\textstyle\prod_v O_v^\times \times F_\infty^\times \longrightarrow C_F := \prod_v'(F_v^\times, O_v^\times) \times F_\infty^\times / F^\times \longrightarrow \mathrm{Cl}_F \longrightarrow 0,.$$

We then have show that

Theorem 3.9. *The ideal class group of a global function field is isomorphic to the Galois group of the maximal abelian unramified extension that is split at all places above infinity.*

On the other hand, by [Ros13, Proposition 14.1], with $S = S_\infty$, we can relate the class group to the Jacobian of the curve C_F corresponding to F via

$$\mathrm{Cl}_F^0 \to \mathrm{Cl}_F \to \mathbb{Z}/(d/i)\mathbb{Z} \to 0, \tag{3.20}$$

where $d = \gcd_{v|\infty}\{\deg(v)\}$ and $i = \gcd_v\{\deg(v)\}$, and $\mathrm{Cl}_F^0 = \mathrm{Jac}(C_F)(\mathbb{F}_q)$ is the Picard group. This means that we can bound $|\mathrm{Cl}_F[\ell]| \le O(\ell^{2g})$ by the structure of Jacobian.

Lemma 3.10. *For any finite function field $F/\mathbb{F}_q(t)$, we have $|\mathrm{Cl}_F[\ell]| \le O_\ell(\ell^{2g})$.*

Lemma 3.11. *Let Q be a finite extension over $\mathbb{F}_q(t)$ and ℓ be a prime that is relatively prime to q. We then have*

$$N_Q(C_\ell, X) = O(C(\ell)^{2g}) X^{1/a(C_\ell)} \ln^{b(C_\ell,Q)-1} X,$$

where the constant $C(\ell)$ only depends on ℓ.

Proof. Denote $a = a(C_\ell)$ and $b = b(C_\ell, Q)$ for short in the proof. It follows from class field theory over function field that

$$N_k(C_\ell, q^m) \leq O(\ell^{2g(k)}) \cdot \mathrm{Hom}_{\leq X}(\prod_v O_v^\times, C_\ell),$$

where $\mathrm{Hom}(\prod_v O_v^\times, C_\ell)$ denotes the number of continuous homomorphisms from $\prod_v O_v^\times$ to C_ℓ with bounded discriminant. It has a generating series which is usually called Malle-Bhargava series. The series is an Euler-product and can be compared to standard zeta functions

$$f(s) := \prod_{|v|\equiv 1 \mod \ell} (1 + (\ell-1)|v|^{-(\ell-1)s}) = H_Q(s) \cdot \zeta_{Q(\mu_\ell)}((\ell-1)s)^{b(C_\ell,F)}. \tag{3.21}$$

Here $H_Q(s)$ is a holomorphic factor that is uniformly converging at $Re(s) > 1/a - \epsilon$ for some small $\epsilon > 0$. Now letting $u = q^{-s}$, we define $g(u) = f(u(s)) = \sum_m a_m u^m$. Since $\zeta_{Q(\mu_\ell)}(s)$ is meromorphic except at its poles, and $H_Q(s)$ is holomorphic at $Re(s) > 1/a - \epsilon$, the complex function $g(u)$ is holomorphic within the disc $|u| < q^{-(1/(\ell-1))}$ and $g(u)/u^{m+1}$ is holomorphic everywhere in the disc except at $u = 0$. We then have for small $0 < \delta < \epsilon$ that

$$2\pi i \cdot a_m = \int_{|u|=q^{-1/(\ell-1)-\delta}} \frac{g(u)}{u^{m+1}} du = \int_{|u|=q^{-1/(\ell-1)+\delta}} \frac{g(u)}{u^{m+1}} du - \sum_{u_0^{\ell-1}=q^{-1}} \mathrm{Res}_{u=u_0} \frac{g(u)}{u^{m+1}}, \tag{3.22}$$

by shifting the contour integration from the smaller circle to the larger circle. The only possible poles for $f(s)$ with $Re(s) > 1/a - \epsilon$ are at s where $q^{as} = q$, i.e., $s_k = 1/a + 2\pi i/a \log q \cdot k$, therefore the possible poles for $g(u)$ are $u(s_k) = q^{-1/a} \cdot \mu_a^k$.

We now estimate the terms in (3.22). The residue of $g(u)/u^{m+1}$ at $u = u(s_k)$ will serve as the main term for a_m. (add -1 since C_1 reversed direction in the second contour integral)

$$\sum_{u_0^{\ell-1}=q^{-1}} \mathrm{Res}_{u=u_0} \frac{g(u)}{u^{m+1}} = (\ln q)^b \frac{(m+b-1)!}{(b-1)!m!} u(s_0)^{-m} \cdot \sum_{k \mod a} \mathrm{Res}(s = s_k) \mu_a^{-km}, \tag{3.23}$$

where $u(s_0) = q^{-1/a}$ and $(m+b-1)!/m!$ is a polynomial of degree $b-1$ in terms of m. The integration can be bounded by

$$\max_{|u|=R=q^{-1/a+\delta}} |g(u)| \cdot R^{-(m+1)} \cdot 2\pi R = O\Big(\max_{|u|=R=q^{-1/a+\delta}} |g(u)| \Big) \cdot q^{(1/a-\delta)m}, \tag{3.24}$$

which is power-saving from the leading terms. The dependence on the base field Q is from $\max_{|u|=R=q^{-1/a+\delta}} |g(u)|$. Here $g(u) = \zeta_{Q(\mu_\ell)}(as)^b$. By [Ros13, Theorem 5.9], we have

$$\zeta_{Q(\mu_\ell)} = \frac{\prod_{1\leq i\leq 2g}(1-\alpha_i q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

where $|\alpha_i| = \sqrt{q}$ and g is the genus. Therefore on $|u| = q^{1/a+\delta}$ we have

$$|g(u)| \leq O(2^{2g}).$$

Combining above, we obtain that there exists $\epsilon > 0$ such that

$$a_m = O(q^{m/a}P(m)) + O(2^{2g}q^{m/a-\epsilon}), \tag{3.25}$$

where the polynomial $P(m)$ has degree at most $b-1$ in m and the constants can be understood by expanding the rational polynomial. Via an explicit computation, we have

$$\zeta_{Q(\mu_\ell)}(s) \sim \prod(1-\alpha_j q^{-s}) \cdot \frac{s-1}{(q^{1-s}-1)(1-q^{-s})} = (\sum b_i(s-1)^i) \cdot (\sum a_j(s-1)^j),$$

where a_j and b_i serve as the coefficients for the Taylor expansion around $s=1$. The a_j does not depend on Q. The polynomial $P(m)$ depends on the first b coefficients of $\zeta_{Q(\mu_\ell)}$. We can compute coefficients b_j via taking derivatives of the ζ-polynomials directly, as an example,

$$b_0 = \prod(1-\alpha_j q^{-1}), \qquad b_1 = b_0 \cdot \sum \alpha_j \ln q \cdot q^{-1}(1-\alpha_j q^{-1})^{-1},$$

similarly, we can compute b_j and obtain that for $0 \le j \le b$

$$b_j = O(C^g)$$

for some constants C only depending on b and g. This finishes the proof for $a_m = O(C^g)q^{m/a}m^{b-1}$. The statement follows by adding up over all $q^m \le X$.

□

Proof of Lemma 3.7. Firstly, it is easy to compute that $b_T(G, \mathbb{F}_q(t)) = \gcd(d, \ell-1)$ by Theorem 2.12 by only considering ϕ exactly corresponding to cyclotomic subfields of $\mathbb{F}_q(t)(\mu_\ell)$.

Next in order to show it is the true counting, it suffices to prove the equality 3.18 from previous discussion, i.e., give the inductive argument for this case.

We need to firstly show that the number of C_ℓ-extensions L/F with $\mathrm{Gal}(L/\mathbb{F}_q(t)) = C_\ell \wr C_d$ for each C_d-extension $F/\mathbb{F}_q(t)$ is bounded from above and below by $X^{1/a(C_\ell)} \ln^{b(C_\ell,F)-1} X$. It is clear from Theorem 3.8 that the upper bound holds. Let v be a place in $\mathbb{F}_q(t)$ that becomes split in F, and $v = \prod_i w_i$. The number of C_ℓ-extensions that are ramified at w_1 and unramified at all other w_i can be counted by [Wri89, Theorem 7.2, Theorem] (together with the remarks after Theorem 7.3), and has a leading term with the same order with the total counting. All extensions satisfying this local condition have total Galois group $C_\ell \wr C_d$, since the Frobenius at v generate C_ℓ^d in $C_\ell \wr C_d$. This implies that the lower bound for $N(G,X)$ is $X^{1/a} \ln^{b-1} X$ where $b = \max_F b(C_\ell, F)$.

Secondly, we need to show that we can add up each counting over all F. With the uniformity proven in Lemma 3.10, we have that

$$N(G,X) \le \sum_F N_F(C_\ell, X/\operatorname{Disc}(F)^\ell) = \sum_F O((C)^{g(F)} \operatorname{Disc}(F)^{-\ell}) X^{1/a} \ln^{b-1} X,$$

where

$$O(\sum_F (C)^{g(F)} q^{-\ell(2g-2)}) = O(1),$$

as long as q is large enough comparing to ℓ. Therefore we prove $N(G,X)$ has an upper bound and lower bound with the same order

$$a = a(C_\ell), \qquad b = \max_F b(C_\ell, F).$$

□

4 Embedding Cyclotomic Extension

In this section, we would like to consider Problem 1.2. Precisely, given a surjective group homomorphism $\pi : G \to B$ and a cyclotomic B-extension F/Q (equivalently a surjective continous group homomorphism $\phi : G_Q \to B$), we say the embedding problem $\mathscr{E}(G_Q, \phi, \pi)$ is *solvable* if there exists a continuous group homomorphism $\tilde{\phi}$ so that the following diagram commutes. We say $\mathscr{E}(G_Q, \phi, \pi)$ is *properly solvable* if moreover $\tilde{\phi}$ is surjective.

$$\begin{array}{ccccccccc} & & & & & & G_Q & & \\ & & & & & \overset{\tilde{\phi}}{\swarrow} & \downarrow \phi & & \\ 0 & \longrightarrow & \mathrm{Ker}(\pi) & \longrightarrow & G & \xrightarrow{\pi} & B & \longrightarrow & 0 \end{array}$$

We are going to see that the crucial difference between global function fields and number fields is that $\mathrm{Gal}(Q^{cyc}/Q)$ is projective for function fields, but not for number fields! Theorem 4.1 and Theorem 4.2 serves the purpose to give a flavor of this question on two sides. As these questions are studied a lot but not from this perspective, we do not claim they are novel from the perspective of technology or strength.

4.1 Function Field

Theorem 4.1. *Let Q be a global function field with maximal constant field $\mathbb{F}_q$. For any cyclotomic B-extension $\phi : G_Q \twoheadrightarrow B$ and a surjective group homomorphism $\pi : G \to B$. We have $\mathscr{E}(G_Q, \phi, \pi)$ is always solvable. If $(\mathrm{Ker}(\phi), q(q-1)) = 1$ and $\mathrm{Ker}(\phi)$ is solvable, then $\mathscr{E}(G_Q, \phi, \pi)$ is always properly solvable.*

Proof. Firstly, by [NSW08, Corollary (9.5.8)], it suffices to show that $\mathscr{E}(G_Q, \phi, \pi)$ is solvable. We are going to show that it is always solvable. Notice that we can decompose $\phi = \phi_1 \circ \phi_0$ as a composition of ϕ_0 and ϕ_1, therefore it suffices to show that $\mathscr{E}(G_Q^{cyc}, \phi_1, \pi)$ is solvable.

$$\begin{array}{ccccccccc} & & & & & & G_Q & & \\ & & & & & & \downarrow \phi_0 & & \\ & & & & & & G_Q^{cyc} & & \\ & & & & & \overset{\tilde{\phi_1}}{\swarrow} & \downarrow \phi_1 & & \\ 0 & \longrightarrow & \mathrm{Ker}(\pi) & \longrightarrow & G & \xrightarrow{\pi} & B & \longrightarrow & 0 \end{array}$$

The group $G_Q^{cyc} \simeq \hat{\mathbb{Z}}$ is a projective profinite group, therefore $\mathscr{E}(G_Q^{cyc}, \phi_1, \pi)$ is always solvable. □

4.2 Number Field

What makes the key difference between function fields and number fields is that $G_{\mathbb{Q}}^{cyc}$ is no longer projective as a profinite group, therefore it is not always possible to embed a cyclotomic extension into a bigger G-extension. In general, it is a difficult question whether $\mathscr{E}(G_Q, \phi, \pi)$ is solvable for a given ϕ and π. In this section, we give a full criteria for $\mathscr{E}(G_Q, \phi, \pi)$ when G is abelian and Q is an arbitrary number field.

Notice that for each place v of Q, the map ϕ induces a local map $\phi_v : G_{Q_v}^{ab} \to G_Q^{ab} \to B$, therefore induces a local embedding problem $\mathscr{E}(G_{Q_v}^{ab}, \phi_v, \pi)$. Central embedding problems satisfy a local-global principle, i.e., $\mathscr{E}(G_Q, \phi, \pi)$ is solvable if and only if $\mathscr{E}(G_{Q_v}, \phi_v, \pi)$ is solvable at each v, see [MM99, Corollary 10.2].

Theorem 4.2. *Let G be an abelian group and Q be a number field. The problem $\mathscr{E}(G_Q, \phi, \pi)$ is properly solvable if and only if $\mathscr{E}(\mu(Q_v), \phi_v, \pi)$ is solvable at each ramified v.*

Proof. By [MM99, Corollary 10.2], $\mathscr{E}(G_Q, \phi, \pi)$ is properly solvable if and only if $\mathscr{E}(G_{Q_v}, \phi_v, \pi)$ is solvable for any v. By class field theory, for a finite place v, we have $G_{Q_v}^{ab} \simeq \hat{Q_v^\times} \simeq \hat{\mathbb{Z}} \times \mu(Q_v) \times \mathscr{O}_v$ where both $\hat{\mathbb{Z}}$ and $\mathscr{O}_v$ are projective profinite groups. Therefore to solve $\mathscr{E}(G_{Q_v}, \phi_v, \pi)$ it suffices to solve $\mathscr{E}(\mu(Q_v), \phi_v, \pi)$. □

Example 4.3. *Let $Q = \mathbb{Q}$, an odd prime ℓ, and $d > 0$. Let $n | \gcd(d, \ell - 1)$, and $B = C_n$ and $\phi : G_{\mathbb{Q}} \to C_n$ corresponds to the unique C_n-sub extension F contained in $\mathbb{Q}(\mu_\ell)$. By Theorem 4.2, it suffices to check the local solvability by $v = \ell$ and $v = \infty$. Notice that $(\ell, \ell - 1) = 1$, the prime ℓ is totally tamely ramified in F. The local map ϕ_v then maps $\mu(\mathbb{Q}_\ell) = \{\mu_{\ell-1}\} \simeq \mathbb{Z}/(\ell - 1)\mathbb{Z}$ by sending the generator to generator of C_n. In order to lift ϕ, the only way is to map the generator of $\mu(\mathbb{Q}_\ell)$ to $g \in C_d$ such that $\bar{g}$ generate C_n and $(\ell - 1)g = 0$. Writing $d = \prod_i p_i^{r_i}$, $\ell - 1 = \prod_i p_i^{u_i}$, $\gcd(d, \ell - 1) = \prod_i p_i^{s_i}$ and $n = \prod_i p_i^{t_i}$. We consider all abelian groups here as a direct product of cyclic p_i-groups. If $\phi(g_i) = 1$ for every $p_i | n$, then we need $(\ell - 1)g_i = 0$ for a generator g_i in C_d, equivalently, this means that $u_i \geq r_i$. At $v = \infty$, if ϕ is totally real, i.e., $n | (\ell - 1)/2$, then always solvable. If $n \nmid (\ell - 1)/2$, then it suffices that $2g_i = 0$ and $\phi(g_i)$ has order 2. This requires 2-Sylow subgroup for C_d and C_n being the same.*

5 Acknowledgement

The author was partially supported by Foerster-Bernstein Fellowship at Duke University and NSF grant DMS-2201346. A significant part of this work is done during my graduate school, so I would like to thank my advisor Melanie Matchett Wood for many inspiring questions and helpful discussions on the topic, especially on understanding the statement of Türkelli's modification. I would also like to thank Brandon Alberts, Jürgen Klüners, Aaron Landsman, Robert J. Lemke Oliver, Yuan Liu and Bianca Viray for helpful conversations.

References

[Alb22] Brandon Alberts. Statistics of the first galois cohomology group: a refinement of malle's conjecture. *Algebra & Number Theory*, 15(10):2513–2569, 2022.

[AO21] Brandon Alberts and Evan O'Dorney. Harmonic analysis and statistics of the first galois cohomology group. *Research in the Mathematical Sciences*, 8(3):50, 2021.

[AOWW24] Brandon Alberts, R.J. Lemke Oliver, J. Wang, and M. M. Wood. Inductive methods for counting number fields. *preprint*, 2024.

[ASVW21] S. Ali Altuğ, Arul Shankar, Ila Varma, and Kevin H. Wilson. The number of D_4-fields ordered by conductor. *J. Eur. Math. Soc. (JEMS)*, 23(8):2733–2785, 2021.

[BF10] K. Belabas and E. Fouvry. Discriminants cubiques et progressions arithmetiqués,. *Int. J. Number Theory*, 6(7):1491–1529, 2010.

[Bha05] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math.*, 162(2):1031–1063, September 2005.

[Bha10] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[BLJ20] Alex Bartel and Hendrik W Lenstra Jr. On class groups of random number fields. *Proceedings of the London Mathematical Society*, 121(4):927–953, 2020.

[BW08] M. Bhargava and M. M. Wood. The density of discriminants of S_3-sextic number fields. *Proc. Amer. Math. Soc.*, 136(5):1581–1587, 2008.

[CyDO02] H. Cohen, F. Diaz y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.*, 133(1):65–93, 2002.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London. Ser. A*, 322(1551):405–420, 1971.

[DW88] B. Datskovsky and D. J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math*, (386):116–138, 1988.

[ETW17] J. Ellenberg, T. Tran, and C. Westerland. Fox-Neuwirth-Fuks cells, quantum shuffle algebras and Malle's conjecture for function field. *arXiv: 1701.04541*, 2017.

[EV05] Jordan S Ellenberg and Akshay Venkatesh. Counting extensions of function fields with bounded discriminant and specified galois group. In *Geometric methods in algebra and number theory*, pages 151–168. Springer, 2005.

[Klü05a] J. Klüners. A counter example to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.

[Klü05b] J. Klüners. *Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe.* Shaker Verlag, 2005.

[Klü12] J. Klüners. The distribution of number fields with wreath products as Galois groups. *Int. J. Number Theory*, (8):845–858, 2012.

[KP21] P. Koymans and C. Pagano. On Malle's conjecture for nilpotent gropus, i. *arXiv: 2103.17223*, 2021.

[KP23] Peter Koymans and Carlo Pagano. Malle's conjecture for fair counting functions. *arXiv preprint arXiv:2309.04838*, 2023.

[KW21] J. Klüners and J. Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group. *Proc. Amer. Math. Soc.*, 2021.

[LWZB19] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown. A predicted distribution for galois groups of maximal unramified extensions. *arXiv preprint arXiv:1907.05002*, 2019.

[Mal02] G. Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[Mal04] G. Malle. On the distribution of Galois groups, II. *Experiment. Math.*, 13(2):129–135, 2004.

[MM99] Gunter Malle and Bernd Heinrich Matzat. *Inverse galois theory*. Springer, 1999.

[MTTW20] R. Masri, F. Thorne, W-L Tsai, and J. Wang. Malle's conjecture for $G \times A$ with $G = S_3, S_4, S_5$. *arXiv: 2004.04651*, 2020.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer-Verlag Berlin Heidelberg, 2008.

[PTBW19] Lillian B Pierce, Caroline L Turnage-Butterbaugh, and Melanie Matchett Wood. On a conjecture for ℓ-torsion in class groups of number fields: from the perspective of moments. *arXiv preprint arXiv:1902.02008*, 2019.

[Ros13] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2013.

[ST24] Arul Shankar and Frank Thorne. On the asymptotics of cubic fields ordered by general invariants. *Commentarii Mathematici Helvetici*, 2024.

[Tür15] Seyfi Türkelli. Connected components of hurwitz schemes and malle's conjecture. *Journal of Number Theory*, 155:163–201, 2015.

[Wan21] J. Wang. Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$. *Compositio Math.*, 2021.

[Woo10] M. M. Wood. On the probabilities of local behaviors in abelian field extensions. *Compositio Math.*, 146(1):102–128, 2010.

[Wri89] D. J. Wright. Distribution of discriminants of abelian extensions. *Proc. of London Math. Soc. (3)*, 58(1):1300–1320, 1989.

Jiuya Wang, Department of Mathematics, University of Georgia, GA 30602, USA
E-mail address: jiuya.wang@uga.edu