COUNTING TOWERS OF NUMBER FIELDS
VIA GALOIS COHOMOLOGY

BRANDON ALBERTS

These are notes for a talk given at the Boston-Keio conference on Number Theory in June 2019. The talk is based on original research found in [Alb19], and this document is a simplified version of the introduction to that paper.

1. Introduction to Malle’s Conjecture

Number field counting problems began by asking questions about how many number fields there are with bounded discriminant. In the study of this topic, the problem naturally partitioned into counting number fields with prescribed Galois group. Malle [Mal02] [Mal04] collected this problem together under the roof of a single conjecture. Let \( K \) be a number field and \( G_K = \text{Gal}(\overline{K}/K) \) be its absolute Galois group throughout the paper. If \( L/K \) is a degree \( n \) extension, we refer to the Galois group \( \text{Gal}(L/K) \subset S_n \) as the Galois group of the Galois closure of \( L/K \) together with the action permuting the \( n \) embeddings of \( L \) into the algebraic closure \( \overline{K} \). If \( G \subset S_n \) is a transitive permutation group, we may ask how many degree \( n \) extensions \( L/K \) there are with \( \text{Gal}(L/K) \cong G \) and bounded discriminant, i.e. what is the size of the counting function

\[
N(K, G; X) := \# \{ L/K : [L : K] = n, \text{Gal}(L/K) \cong G, N_{K/Q}(\text{disc}(L/K)) < X \}.
\]

Malle gave theoretical evidence suggesting how this function should grow asymptotically as \( X \) tends to infinity. This is often referred to as the “Strong Form” of Malle’s conjecture.

**Conjecture 1.1** (Strong Form of Malle’s Conjecture). Let \( G \subset S_n \) be a transitive subgroup and define the class function \( \text{ind} : G \to \mathbb{Z} \) by \( \text{ind}(g) = n - \#\{ \text{orbits of } g \} \). Then

\[
N(K, G; X) \sim c(K, G)X^{1/a(C)}(\log X)^{b(K, G)-1},
\]

where \( a(G) = \min_g \# \neq 1 \text{ ind}(g) \) and

\[
b(K, G) = \# \{ \text{conjugacy class } C \subset G : \text{ind}(C) = a(G) \} / \chi
\]

is the number of orbits under the action by the cyclotomic character \( \chi : G_K \to \hat{\mathbb{Z}} \) on the set of conjugacy classes, where the action is given by \( \sigma.g = g^{\chi(\sigma)} \).

This conjecture is known to be true for several families of groups including abelian groups \( A \) [Wri89], \( S_n \) for \( n = 3, 4, 5 \) [DW88, BSW15], \( A \times S_n \) for \( n = 3, 4, 5 \) and \( |A| \) coprime to \( 2, 12, 60 \) respectively [Wan17], and certain wreath products by abelian groups or \( S_3 \) [LOWW19]. However, for the majority of groups not much is known. To complicate matters, the conjecture is known to be false by a counter example due to Klüners for \( G = C_3 \wr C_2 \) [Kli05].

A weaker version of this conjecture asserts that merely the power of \( X \) is correct. This is known for more cases, notably including all nilpotent groups in the regular representation [KM04]. Nontrivial upper bounds given as a power of \( X \) are known for all groups, while nontrivial lower bounds given as a power of \( X \) are known for certain families of groups.
2. Inductive Methods

One of the modern approaches to Malle’s conjecture that we will focus on is inductively counting extensions. These methods are used to prove Malle’s conjecture in the only large families of nonabelian groups for which the conjecture is known, and are outlined in detail in an upcoming preprint of Lemke Oliver-Wang-Wood \([LOWW19]\). Fix a finite group \(G\), and say we want to count \(G\)-extensions \(F/K\) ordered by some invariant. If \(G\) is not a simple group, we could potentially break down this counting problem into two separate counting problems. We adopt the very intuitive notation introduced in an upcoming preprint by Lemke Oliver-Wang-Wood \([LOWW19]\). Suppose \(T \trianglelefteq G\) is a normal subgroup with quotient group \(G/T = B\). Any \(G\)-extension \(F/K\) decomposes into a tower of fields:

\[
\begin{array}{c}
F \\
\downarrow T \\
L \\
\downarrow B \\
K
\end{array}
\]

(1)

We may think of “\(T\)” as standing for “top extension” and “\(B\)” as standing for “bottom extension” to help us keep track of the notation. This approach to Malle’s Conjecture breaks the counting problem into two steps:

1. Let \(\alpha\) be the isomorphism class of the extension

\[
1 \longrightarrow T \longrightarrow G \longrightarrow B \longrightarrow 1
\]

Denote by \(N(L/K, \alpha; X)\) the number of towers \([1]\) with \(\text{disc}(F/K) \leq X\) and a fixed bottom extension \(L/K\) together with an isomorphism \(\text{Gal}(F/K) \xrightarrow{\sim} G\) which make the short exact sequence of Galois groups isomorphic to \(\alpha\). How does \(N(L/K, \alpha; X)\) grow as \(X\) tends towards \(\infty\)?

2. Compute the summation over the choices of bottom extension \(L/K\)

\[
\sum_{L/K} N(L/K, \alpha; X).
\]

This is equal to \(N(K, G; X)\) by construction.

Each of these steps comes with a major obstacle. For Step 1 we can count \(T\)-extension \(F/L\) as in Malle’s Conjecture, and the major obstacle is controlling for the Galois group of the whole tower \(\text{Gal}(F/K)\). For Step 2, just because we know the answer for step 1 does not mean we know how to sum those counting functions together. The major obstacle is to improve the counting results from Step 1 to be uniform in the choice of bottom extension \(L/K\), which allows for better control of the error term.

3. Main Results

This talk will focus on Step 1. We do not aim to say anything about the inverse Galois problem, so suppose that at least one such tower containing a fixed bottom extension \(L/K\) exists, given by the surjective homomorphism \(\pi : G_K \twoheadrightarrow G\).
Lemma 3.1. Let $T^n$ be the group $T$ with the Galois action $x.t = t^{\pi(x)}$. Then
\[ N(L/K, \alpha; X) = \# \{ f \in Z^1(G_K, T^n) : f * \pi \text{ surjective, } \text{disc}(f * \pi) \leq X \}, \]
where $(f * \pi)(x) = f(x)(\pi(x))$.

In particular, we can write this statement as
\[ N(L/K, \alpha; X) = \text{surjective elements of } Z^n_\pi(K, T^n) \text{ with discriminant } \leq X. \]

We can think of this as a direct generalization to classical number field counting problems and Malle’s conjecture, where Malle predicts the growth of
\[ N(K, T; X) = \text{surjective elements of } \text{Hom}(G_K, T) \text{ with discriminant } \leq X \]
when $T$ has the trivial Galois action.

In fact, these counting functions are so similar that we can extrapolate the heuristic justifications of Malle’s conjecture to make a prediction for this behavior. In particular, we prove that the Malle-Bhargava principle [Bha10] [Woo17] gives the following prediction to this generalized question:

**Malle-Bhargava Prediction.** Fix $G \subseteq S_n$, $T \subseteq G$, and $\pi : G_K \to G$ a homomorphism. Define the class function $\text{ind}(g) = n - \# \{ \text{orbits of } g \}$. Then
\[ N(L/K, \alpha; X) \sim c(K, T)X^{1/a(T)}(\log X)^{b(K, T^n) - 1}, \]
where $a(T) = \min_{t \in T \setminus \{1\}} \text{ind}(t)$ and
\[ b(K, T^n) = \# \{ \text{conjugacy class } C \subseteq T : \text{ind}(C) = a(T) \}/\pi * \chi^{-1} \]
is the number of orbits under the composite action given by $\pi$ and the cyclotomic character $\chi : G_K \to \hat{\mathbb{Z}}$ on the set of conjugacy classes, where the action is given by $\sigma.g = g^{\pi(\sigma)\chi(\sigma)^{-1}}$.

The invariants $a(T)$ and $b(K, T^n)$ exactly correspond to Malle’s predicted invariants, where we make sure to account for the extra “conjugates” under the Galois action by $\pi$.

Of course, Malle’s conjecture has known counter examples (such as $G = C_3 \wr C_2$), so it is reasonable to be suspicious of any generalization of the conjecture and its justifications.

To lend more credence to the idea that something of this form should be true, we prove it in a special case:

**Theorem 3.2.** Fix $G \subseteq S_n$ a transitive subgroup, $T \subseteq G$ an abelian normal subgroup with $B := G/T$, and $\alpha \in H^2(B, T)$. If $L/K$ is a fixed $B$-extension and there exists at least one tower of the form [4] given by $\pi : G_K \to G$, then
\[ N(L/K, \alpha; X) \sim c(K/L, \alpha)X^{1/a(T)}(\log X)^{b(K, T^n) - 1}, \]
verifying the Malle-Bhargava prediction.

The next step for applying inductive methods would be to prove this theorem (or possibly a weaker statement) is uniform in the choice of base field $L/K$. However, without performing any extra work we can use this result to give nontrivial lower bounds for $N(K, G; X)$ for groups $G$ that have an abelian normal subgroup. Every such tower is necessarily a $G$-extension, which implies that if $G$ has an abelian normal subgroup and the inverse Galois problem is solved for $G$ then
\[ N(K, G; X) \geq N(L/K, \alpha; X). \]

What is a large family of groups with abelian normal subgroups for which the inverse Galois problem is solved? Solvable groups!
Corollary 3.3. For any solvable transitive subgroup $G \subseteq S_n$ and any number field $K$, there exists an integer $0 < a < n$ depending only on $G$ such that

$$N(K, G; X) \gg X^\frac{a}{n}.$$ 

In particular, we can take

$$a = \min \{ \text{ind}(g) : g \in G - \{1\} \text{ and } g \text{ commutes with its conjugates} \}.$$ 

For many solvable groups this is the first known nontrivial lower bound, and is at least as large as $X^{\frac{1}{n-1}}$.

References


