Galois Cohomology and Number Field Counting

Brandon Alberts (University of Wisconsin-Madison)

University of Wisconsin-Madison

August 7, 2018
1 Introduction

2 Weak Malle and Solvable Groups

3 Example: Nonabelian Cohen-Lenstra Moment

4 Lemmermeyer Factorizations and the Future
For $K$ a number field and $G \subseteq S_n$ a transitive permutation group, define

$$N(K, G; X) = \#\{L/K : \text{Gal}(L/K) \cong G, \mathcal{N}_{K/Q}(D_{L/K}) < X\}$$

### Conjecture (Strong Form)

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

### Conjecture (Weak Form)

$$\lim_{X \to \infty} \frac{\log N(K, G; X)}{\log X} = \frac{1}{a(G)}$$
## Malle’s Conjecture Known Cases

Key: SF=Strong Form, WF=Weak Form, WFL=Weak Form Lower Bound, WFU=Weak Form Upper Bound

<table>
<thead>
<tr>
<th>Groups</th>
<th>Known</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abelian</td>
<td>SF</td>
<td>Wright [16] ‘89</td>
</tr>
<tr>
<td>Degree $n$</td>
<td>$\leq \frac{n+2}{4}$</td>
<td>Schmidt [13] ‘95</td>
</tr>
<tr>
<td>$D_\ell$</td>
<td>WF*</td>
<td>Klüners [9] ‘06</td>
</tr>
<tr>
<td>$S_3 \subset S_6$</td>
<td>SF</td>
<td>Bhargava-Wood [2] ‘07</td>
</tr>
<tr>
<td>Degree $n$</td>
<td>$\leq \exp(C\sqrt{\log n})$</td>
<td>Ellenberg-Venkatesh [6] ‘10</td>
</tr>
<tr>
<td>$C_2 \wr H$</td>
<td>SF</td>
<td>Klüners [10] ‘12</td>
</tr>
<tr>
<td>$S_3, S_4, S_5$</td>
<td>SF</td>
<td>Bhargava [1] ‘14</td>
</tr>
<tr>
<td>$A \times S_n$, $n = 3, 4, 5$</td>
<td>SF</td>
<td>Wang [15] ‘17</td>
</tr>
<tr>
<td>$G \neq S_n$</td>
<td>$\leq \frac{\sum_{i=1}^{n-1} \deg(f_{i+1}) - [K:Q]^{-1}}{2(n-t)}$</td>
<td>Dummit [4] ‘18</td>
</tr>
</tbody>
</table>

*Conditional on Cohen-Lenstra heuristics, unconditionally $\leq \frac{3}{2a(D_\ell)}$. 
Cohen-Lenstra Moments

Fix a pair of groups \((G, G')\) and \(\mathcal{Q}_X^\pm\), the set of real/imaginary quadratic fields with discriminant \(\leq X\).

\[
N^\pm(G, G'; X) = \sum_{K \in \mathcal{Q}_X^\pm} \# \{L/K : \text{unram}, (\text{Gal}(L/K), \text{Gal}(L/\mathbb{Q})) \cong (G, G') \}
\]

**Conjecture (Wood)**

*If \((G, G')\) admissible and good, then*

\[
N^\pm(G, G'; X) \sim c^\pm(G, G')X
\]

*for an explicit positive constant \(c^\pm(G, G')\). If \((G, G')\) admissible and not good then*

\[
\lim_{X \to \infty} \frac{N^\pm(G, G'; X)}{X} = \infty
\]
## Cohen-Lenstra Moments Known Cases

<table>
<thead>
<tr>
<th>Pair</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(C_2^n, C_2^{n+1})$</td>
<td>genus theory</td>
</tr>
<tr>
<td>$(C_4^n, C_4^n \times C_2)$</td>
<td>Fouvry-Klüners [7] ‘07</td>
</tr>
<tr>
<td>$(A_n, S_n), n = 3, 4, 5$</td>
<td>Bhargava [1] ‘14</td>
</tr>
<tr>
<td>$(S_n, S_n \times C_2)$</td>
<td>Bhargava [1] ‘14</td>
</tr>
<tr>
<td>$(A, A \times C_2), A = \text{fin. ab. 2-gp.}$</td>
<td>Smith [14] ‘17</td>
</tr>
</tbody>
</table>
A Common Counting Function

Fix a number field $K$ with absolute Galois group $G_K$ and group of fractional ideals $I_K$. Fix an invariant $\text{inv} : \text{Hom}(G_K, G) \to I_K$ that behaves similarly to a discriminant. Fix $\Sigma = (\Sigma_p)$ for $\Sigma_p \subset \text{Hom}(G_{K_p}, G)$. Define

$$N_{\text{inv}}(K, \Sigma; X) = \# \{ \pi : G_K \to G : (\pi|_{G_{K_p}}) \in \Sigma, N_{K/\mathbb{Q}}(\text{inv}(\pi)) \leq X \}$$

The counting function from Malle’s Conjecture is given by $\Sigma_p = \text{Hom}(G_{K_p}, G)$ and

$$N(K, G; X) = \frac{1}{|\text{Aut}(G)|} N_{\text{disc}}(K, \Sigma; X)$$

The counting function for nonabelian Cohen-Lenstra Moments is given by $\Gamma_p = \{ \gamma : G_{\mathbb{Q}_p} \to G' : |\gamma(I_p)| \mid 2, \gamma(I_p) \cap G = 1 \}$, $\Gamma_{\infty}$ depending on $\pm$, $\text{inv}(\pi) = \text{disc}(\text{quad. subfield of } \overline{\mathbb{Q}^{\ker \pi}})$ and

$$N^{\pm}(G, G'; X) = \frac{1}{|\text{Aut}_G(G')|} N_{\text{inv}}(\mathbb{Q}, \Gamma; X)$$
Overarching Question

How does $N_{inv}(K, \Sigma; X)$ behave asymptotically?
1 Introduction

2 Weak Malle and Solvable Groups

3 Example: Nonabelian Cohen-Lenstra Moment

4 Lemmermeyer Factorizations and the Future
A New Upper Bound

**Theorem (A.)**

Let $G$ be a finite solvable group. Then

$$\limsup_{X \to \infty} \frac{\log N_{\text{inv}}(K, \Sigma; X)}{\log X} \leq \frac{1}{a_{\text{inv}}(\Sigma)} \left( 1 + \sum_{\alpha \in A} C_\alpha \limsup_{[L:K] \leq N_\alpha \to \infty} \frac{\log |\text{Cl}(L)[\ell_\alpha]|}{\log D_{L/Q}} \right)$$

for explicit positive constants $C_\alpha$, $N_\alpha$, and explicit primes $\ell_\alpha \mid |G|$ over finitely many indices $\alpha \in A$.

The set of indices $A$ depends on the length of a normal series of $G$ with nilpotent factors. If $G$ is nilpotent then $A = \emptyset$. If $G$ is nearly nilpotent, $A$ is small.
Definition

\[ a_{\text{inv}}(\Sigma) = \lim_{N_{K/Q} \to \infty} \inf \max_{\pi \in \Sigma} \nu_p(\text{inv}(\pi)) \]

In words, this is the largest exponent in the prime factorization of \( \text{inv}(\pi) \) that occurs for infinitely many places \( p \).

This agrees with the invariant given by Malle when \( \Sigma_p = \text{Hom}(G_{K_p}, G) \) is trivial so that

\[ a_{\text{disc}}(\Sigma) = a(G) \]
Unpacking the Upper Bound

**Conjecture**

\[
\lim_{[L:K] \leq N, D_L/Q \to \infty} \frac{\log |\text{Cl}(L)[\ell]|}{\log D_L/Q} = 0
\]

*More commonly written as* \(|\text{Cl}(L)[\ell]| \ll D_{L/Q}^e*.

This conjecture implies the upper bound for the Weak Form of Malle’s conjecture holds for all solvable groups AND generalizes to all \(N_{\text{inv}}(K, \Sigma; X)\) for any solvable group. It is known in only a few cases, such as for \(N = \ell = 2\) by genus theory.

<table>
<thead>
<tr>
<th>Known upper bound</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\frac{1}{2} \quad \frac{1}{2} \quad \frac{1}{2\ell([L:K]-1)})</td>
<td>unconditionally by Minkowski’s bounds conditional on GRH by Ellenberg-Pierce-Wood [5] ‘07</td>
</tr>
</tbody>
</table>
Proof Idea

Consider an exact sequence

\[ 1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1 \]

\[ 1 \rightarrow \text{Hom}(H, N) \rightarrow \text{Hom}(H, G) \rightarrow \text{Hom}(H, G/N) \]

Fix a normal series (i.e. \( G_i \trianglelefteq G \))

\[ 1 = G_0 \leq \cdots \leq G_{m-1} \leq G_m = G \]

Lemma

*There exists \( L_i/K \) such that \([L_i : K]\) bounded independent of \( K \)*

\[ |\text{Hom}(G_K, S, G)| \leq C \prod_{i=1}^{m} |\text{Hom}(G_{L_i}, S, G_i/G_{i-1})| \]
Introduction

Weak Malle and Solvable Groups

Example: Nonabelian Cohen-Lenstra Moment

Lemmermeyer Factorizations and the Future
The Pair

\[ H_8 = \langle a, b, z : a^2 = b^2 = [a, b] = z, z^2 = [a, z] = [b, z] = 1 \rangle \]

For any positive integer \( k \), there exists a unique group \( G'_k \) up to isomorphism with \( [G'_k : H_8^k] = 2 \) making \( (H_8^k, G'_k) \) an admissible pair

\[ G'_k = H_8^k \rtimes \langle \sigma \rangle \]

where \( \sigma \) acts componentwise by \( \sigma(a) = a z, \sigma(b) = b z, \) and \( \sigma(z) = z \). This pair is not good.
The Main Term

Theorem (A.-Klys)

\[
N^-(H_8^k, G'_k; X) \sim \frac{1}{4^k |\text{Aut}_{G'_k}(H_8^k)|} \sum_{0<d<X} 3^{k \omega(d)}
\]

\[
N^+(H_8^k, G'_k; X) \sim \frac{1}{24^k |\text{Aut}_{G'_k}(H_8^k)|} \sum_{0<d<X} 3^{k \omega(d)}
\]

Remark:

\[
\sum_{0<\pm d<X} 3^{k \omega(d)} = c^{\pm} X (\log X)^{3k-1}
\]

where \( c^{\pm} \) is explicitly given as a lengthy Euler product.
Sketch of Proof

Theorem (Lemmermeyer [12])

There exists an unramified extension $M/\mathbb{Q}(\sqrt{d})$ with $\text{Gal}(M/\mathbb{Q}(\sqrt{d})) \cong H_8$ and $\text{Gal}(M/\mathbb{Q}) \cong H_8 \rtimes \langle \sigma \rangle$ if and only if there is a factorization $d = d_1d_2d_3$ satisfying

- $d_1, d_2, d_3$ are coprime quadratic discriminants, at most one of which is negative.
- $\left(\frac{d_1d_2}{p_3}\right) = \left(\frac{d_1d_3}{p_2}\right) = \left(\frac{d_2d_3}{p_1}\right) = 1$ for primes $p_i \mid d_i$

Moreover, for each factorization there are exactly $2^{\omega(d) - 3}$ such extensions.

The number of unramified $H_8$ extensions $M/\mathbb{Q}(\sqrt{d})$ Galois over $\mathbb{Q}$ can be expressed by

$$\frac{1}{8} \sum_{d=d_1d_2d_3} \prod_{p \mid d} \left(1 + \left(\frac{d_1d_2}{p}\right)\right) \left(1 + \left(\frac{d_1d_3}{p}\right)\right) \left(1 + \left(\frac{d_2d_3}{p}\right)\right)$$
Sketch of Proof

Use the same sieve as Fouvry-Klüners [7] did when finding the average value of the 4-rank of the class group of quadratic fields.

\[
f(d) = \frac{1}{8} \sum_{d=d_1d_2d_3 \ p|d} \prod_p \left(1 + \left(\frac{d_1d_2}{p}\right)\right) \left(1 + \left(\frac{d_1d_3}{p}\right)\right) \left(1 + \left(\frac{d_2d_3}{p}\right)\right)
\]

Take the \(k^{th}\) power and expand the sum so that, for \(u \in \{0, 1, \ldots, 5\}^k\),

\[
f(d)^k = \sum_{d=\prod D_u} \prod_{u, v} \left(\frac{D_u}{D_v}\right)^{\Phi_k(u, v)}
\]

**BIG IDEA:** the main term only comes from those terms which cancel out completely by quadratic reciprocity, i.e. if \(D_u, D_v \neq 1\) then \(\Phi_k(u, v) = \Phi_k(v, u)\) so that the main term is

\[
\sum_{d=\prod D_u} \prod (-1)^{\Phi_k(u, v)} \left(\frac{D_u-1}{2}\right) \left(\frac{D_v-1}{2}\right)
\]
1. Introduction
2. Weak Malle and Solvable Groups
3. Example: Nonabelian Cohen-Lenstra Moment
4. Lemmermeyer Factorizations and the Future
Theorem (Lemmermeyer [12])

There exists an unramified extension $M/\mathbb{Q}(\sqrt{d})$ with $\text{Gal}(M/\mathbb{Q}(\sqrt{d})) \cong H_8$ and $\text{Gal}(M/\mathbb{Q}) \cong H_8 \rtimes \langle \sigma \rangle$ if and only if there is a factorization $d = d_1 d_2 d_3$ satisfying

- $d_1, d_2, d_3$ are coprime quadratic discriminants, at most one of which is negative.
- $\left(\frac{d_1 d_2}{p_3}\right) = \left(\frac{d_1 d_3}{p_2}\right) = \left(\frac{d_2 d_3}{p_1}\right) = 1$ for primes $p_i | d_i$

Moreover, for each factorization there are exactly $2^\omega(d) - 3$ such extensions.
Let $(G, G')$ be an admissible pair with

\[
1 \longrightarrow A \longrightarrow G' \longrightarrow C_2^n \longrightarrow 1
\]

such that $A \subseteq Z(G')$, $A = \Phi(G')$ the Frattini subgroup, $A = C_2^m$. Fix an inner product $\cdot$ on $A$ as an $\mathbb{F}_2$-vector space.
Theorem (A.)

There exists an unramified extension \( M/\mathbb{Q}(\sqrt{d}) \) with \( \text{Gal}(M/\mathbb{Q}(\sqrt{d})) \cong G \) and \( \text{Gal}(M/\mathbb{Q}) \cong G' \) if and only if there is a factorization \( d = \prod_{y \in Y} d_y \) satisfying

- \( Y = \{ gA \in G'/A - G/A : g^2 = 1 \} \)
- \( \{d_y\} \) are coprime quadratic discriminants, such that \( \sum_{d_y < 0} y \in Y \)
- \[
\prod_{y \in Y} \left( \frac{d_y}{p_x} \right)^{v \cdot [y, x]_{G'}} = 1
\]

for all \( x \in Y, p_x | d_x, v \in A \) where \([,]_{G'} : G'/A \times G'/A \to A\) is the commutator of \( G' \).

Moreover, for each factorization there are exactly \(|A|^\omega(d) - n\) such extensions.
The embedding problem on the following central extension

\[
\begin{array}{ccc}
G_{\mathbb{Q}} & \xrightarrow{f} & C_2^n \\
\sim & \downarrow{f} & \\
1 & \longrightarrow & A & \longrightarrow & G' & \longrightarrow & C_2^n & \longrightarrow & 1
\end{array}
\]

has an (unramified) solution exactly when the local embedding problems

\[
\begin{array}{ccc}
G_{\mathbb{Q}_p} & \xrightarrow{f_p} & C_2^n \\
\sim & \downarrow{f} & \\
1 & \longrightarrow & A & \longrightarrow & G' & \longrightarrow & C_2^n & \longrightarrow & 1
\end{array}
\]

all have (unramified) solutions with \(\tilde{f}_p(G_{\mathbb{Q}_p})\) abelian.
Ideas Behind Proof

This lift is unramified if \( \tilde{f}_p(l_p) \) and \( f(l_p) \) have the same cardinality. In particular, a generator of \( l_p(\mathbb{Q}^{ab}/\mathbb{Q}) \) must be sent to some \( x \in Y \). The factors \( d_x \) are determined exactly by which \( p \) have \( \langle f(l_p) \rangle = \langle x \rangle \).

\( \tilde{f}_p(G_{\mathbb{Q}_p}) \) is abelian if and only if \( [f(Frob_p), x]_{G'} = 0 \). Kronecker-Weber gives an explicit description of \( f(Frob_p) \) as a sum of generators \( \tau_q \in l_q(\mathbb{Q}^{ab}/\mathbb{Q}) \)

\[
\sum_q \chi_q(p)f(\tau_q) = \sum_y \left( \sum_{q|d_y} \chi_q(p) \right) y
\]

for \( \left( \frac{q}{p} \right) = (-1)^{\chi_q(p)} \).
Ideas Behind Proof

Given a factorization, use the inflation-restriction sequence to count the number of extensions

\[ 0 \rightarrow H^1(C_2^n, A) \xrightarrow{\inf} H^1(Gal(H_L/Q), A) \xrightarrow{\text{res}} H^1(Cl(L), A) \xrightarrow{\delta} H^2(C_2^n, A) \]

where \( L = \overline{Q}^{\ker f} \). The number of such extensions is in one-to-one correspondence with \( \delta^{-1}([G']) \), which has size

\[ |\ker \delta| = \frac{|H^1(Gal(H_L/Q), A)|}{|H^1(C_2^n, A)|} \]
Thanks for coming!!
Bibliography I

M. Bhargava.

M. Bhargava and M. M. Wood.

H. Davenport and H. Heilbronn.

E. Dummit.

J. S. Ellenberg and A. Venkatesh.

J. S. Ellenberg and A. Venkatesh.
E. Fouvry and J. Klüners.
On the 4-rank of class groups of quadratic number fields.

J. Klüners.
A counter example to Malle’s conjecture on the asymptotics of discriminants.

J. Klüners.
Asymptotics of number fields and the Cohen-Lenstra heuristics.

J. Klüners.
The distribution of number fields with wreath products as Galois groups.

J. Klüners and G. Malle.
Counting nilpotent Galois extensions.

F. Lemmermeyer.
Unramified quaternion extensions of quadratic number fields.
Bibliography III

W. M. Schmidt.
Number fields of given degree and bounded discriminants.

A. Smith.
$2^\infty$-selmer groups, $2^\infty$-class groups, and Goldfeld's conjecture, Feb 2017.

J. Wang.
Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$, Oct 2017.

D. J. Wright.
Distribution of discriminants of abelian extensions.