Counting nilpotent extensions

Peter Koymans
University of Michigan

Arithmetic Statistics

Luminy, 19 May 2023

Malle's conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $a(G) \in \mathbb{Q}_{>0}$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $c(G) > 0$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

Malle's conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $a(G) \in \mathbb{Q}_{>0}$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $c(G) > 0$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

This is a generalization of the inverse Galois problem.

Malle's conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $a(G) \in \mathbb{Q}_{>0}$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $c(G) > 0$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

This is a generalization of the inverse Galois problem.

As phrased above, this conjecture is widely believed to be correct.

Malle's conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $a(G) \in \mathbb{Q}_{>0}$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $c(G) > 0$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

This is a generalization of the inverse Galois problem.

As phrased above, this conjecture is widely believed to be correct.

Malle proposed some explicit values $a_{\mathrm{Malle}}(G)$ and $b_{\mathrm{Malle}}(G)$. Malle's $b_{\mathrm{Malle}}(G)$ is known to be wrong in general.

Malle's conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $a(G) \in \mathbb{Q}_{>0}$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $c(G) > 0$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

This is a generalization of the inverse Galois problem.

As phrased above, this conjecture is widely believed to be correct.

Malle proposed some explicit values $a_{\mathrm{Malle}}(G)$ and $b_{\mathrm{Malle}}(G)$. Malle's $b_{\mathrm{Malle}}(G)$ is known to be wrong in general.

Sometimes $c(G)$ is an Euler product. This is expected to be true for S_n (Malle–Bhargava principle).

An exercise about hyperbolas

We have

$$\sum_{ab^2 \le X} 1 = \sum_{b \le \sqrt{X}} \sum_{a \le X/b^2} 1 = \sum_{b \le \sqrt{X}} \left(\frac{X}{b^2} + O(1) \right)$$
$$= X \sum_{b=1}^{\infty} \frac{1}{b^2} + O(\sqrt{X}).$$

An exercise about hyperbolas

We have

$$\sum_{ab^2 \le X} 1 = \sum_{b \le \sqrt{X}} \sum_{a \le X/b^2} 1 = \sum_{b \le \sqrt{X}} \left(\frac{X}{b^2} + O(1) \right)$$
$$= X \sum_{b=1}^{\infty} \frac{1}{b^2} + O(\sqrt{X}).$$

Observations:

- main contribution comes from $b < \log \log \log \log X$;

An exercise about hyperbolas

We have

$$\sum_{ab^2 \le X} 1 = \sum_{b \le \sqrt{X}} \sum_{a \le X/b^2} 1 = \sum_{b \le \sqrt{X}} \left(\frac{X}{b^2} + O(1) \right)$$
$$= X \sum_{b=1}^{\infty} \frac{1}{b^2} + O(\sqrt{X}).$$

Observations:

- main contribution comes from $b < \log\log\log\log X$;
- every given b contributes a positive proportion to the main term.

An exercise about hyperbolas

We have

$$\sum_{ab^2 \le X} 1 = \sum_{b \le \sqrt{X}} \sum_{a \le X/b^2} 1 = \sum_{b \le \sqrt{X}} \left(\frac{X}{b^2} + O(1) \right)$$
$$= X \sum_{b=1}^{\infty} \frac{1}{b^2} + O(\sqrt{X}).$$

Observations:

- main contribution comes from $b < \log\log\log\log X$;
- every given b contributes a positive proportion to the main term.

An exercise about hyperbolas

We have

$$\sum_{ab^2 \le X} 1 = \sum_{b \le \sqrt{X}} \sum_{a \le X/b^2} 1 = \sum_{b \le \sqrt{X}} \left(\frac{X}{b^2} + O(1) \right)$$
$$= X \sum_{b=1}^{\infty} \frac{1}{b^2} + O(\sqrt{X}).$$

Observations:

- main contribution comes from $b < \log\log\log\log X$;
- every given b contributes a positive proportion to the main term.

Compare instead with

$$\sum_{ab \le X} 1 = \sum_{b \le X} \sum_{a \le X/b} 1 = \sum_{b \le X} \left(\frac{X}{b} + O(1) \right) = X \log X + O(X).$$

An exercise about hyperbolas

We have

$$\sum_{ab^2 \le X} 1 = \sum_{b \le \sqrt{X}} \sum_{a \le X/b^2} 1 = \sum_{b \le \sqrt{X}} \left(\frac{X}{b^2} + O(1) \right)$$
$$= X \sum_{b=1}^{\infty} \frac{1}{b^2} + O(\sqrt{X}).$$

Observations:

- main contribution comes from $b < \log\log\log\log X$;
- every given b contributes a positive proportion to the main term.

Compare instead with

$$\sum_{ab \le X} 1 = \sum_{b \le X} \sum_{a \le X/b} 1 = \sum_{b \le X} \left(\frac{X}{b} + O(1) \right) = X \log X + O(X).$$

Both observations fail now.

Ramification theory

Let $K/\mathbb{Q}$ be a Galois extension and suppose that p does not divide $[K:\mathbb{Q}]$. Then

$$v_p(D_K) = [K:\mathbb{Q}] \cdot \left(1 - \frac{1}{|\mathcal{I}_p|}\right),$$

where $\mathcal{I}_p$ is an inertia subgroup.

Ramification theory

Let $K/\mathbb{Q}$ be a Galois extension and suppose that p does not divide $[K:\mathbb{Q}]$. Then

$$v_p(D_K) = [K:\mathbb{Q}] \cdot \left(1 - \frac{1}{|\mathcal{I}_p|}\right),$$

where $\mathcal{I}_p$ is an inertia subgroup.

Counting by discriminant has some strong similarities with counting under the hyperbola.

Ramification theory

Let $K/\mathbb{Q}$ be a Galois extension and suppose that p does not divide $[K : \mathbb{Q}]$. Then

$$v_p(D_K) = [K : \mathbb{Q}] \cdot \left(1 - \frac{1}{|\mathcal{I}_p|}\right),$$

where $\mathcal{I}_p$ is an inertia subgroup.

Counting by discriminant has some strong similarities with counting under the hyperbola.

Heuristically: almost all ramified primes p in a typical field $K/\mathbb{Q}$ are such that $|\mathcal{I}_p|$ equals the smallest prime divisor of $[K : \mathbb{Q}]$.

Ramification theory

Let $K/\mathbb{Q}$ be a Galois extension and suppose that p does not divide $[K:\mathbb{Q}]$. Then

$$v_p(D_K) = [K:\mathbb{Q}] \cdot \left(1 - \frac{1}{|\mathcal{I}_p|}\right),$$

where $\mathcal{I}_p$ is an inertia subgroup.

Counting by discriminant has some strong similarities with counting under the hyperbola.

Heuristically: almost all ramified primes p in a typical field $K/\mathbb{Q}$ are such that $|\mathcal{I}_p|$ equals the smallest prime divisor of $[K:\mathbb{Q}]$.

Moral: inertia subgroups tend to "typically" be as small as possible when counting by discriminant.

An example

Example (Non-Galois quartic D_4)

If $L/\mathbb{Q}$ is quartic D_4 with quadratic subfield K, then for all $p \neq 2$

$$v_p(D_L) = \begin{cases} 3 & \text{if } p \text{ is totally ramified} \\ 2 & \text{if } p \text{ is in all other cases} \\ 1 & \text{if } p \text{ is unramified in } K/\mathbb{Q} \text{ but ramifies in the biquadratic} \\ 0 & \text{if } p \text{ is unramified.} \end{cases}$$

An example

Example (Non-Galois quartic D_4)

If $L/\mathbb{Q}$ is quartic D_4 with quadratic subfield K, then for all $p \neq 2$

$$v_p(D_L) = \begin{cases} 3 & \text{if } p \text{ is totally ramified} \\ 2 & \text{if } p \text{ is in all other cases} \\ 1 & \text{if } p \text{ is unramified in } K/\mathbb{Q} \text{ but ramifies in the biquadratic} \\ 0 & \text{if } p \text{ is unramified.} \end{cases}$$

Thus, when we count quartic D_4-extensions, the discriminant has the shape ab^2c^3.

An example

Example (Non-Galois quartic D_4)

If $L/\mathbb{Q}$ is quartic D_4 with quadratic subfield K, then for all $p \neq 2$

$$v_p(D_L) = \begin{cases} 3 & \text{if } p \text{ is totally ramified} \\ 2 & \text{if } p \text{ is in all other cases} \\ 1 & \text{if } p \text{ is unramified in } K/\mathbb{Q} \text{ but ramifies in the biquadratic} \\ 0 & \text{if } p \text{ is unramified.} \end{cases}$$

Thus, when we count quartic D_4-extensions, the discriminant has the shape ab^2c^3.

Observations:

- main contribution comes from quadratic fields K with $D_K < \log\log\log\log X$;

An example

Example (Non-Galois quartic D_4)

If $L/\mathbb{Q}$ is quartic D_4 with quadratic subfield K, then for all $p \neq 2$

$$v_p(D_L) = \begin{cases} 3 & \text{if } p \text{ is totally ramified} \\ 2 & \text{if } p \text{ is in all other cases} \\ 1 & \text{if } p \text{ is unramified in } K/\mathbb{Q} \text{ but ramifies in the biquadratic} \\ 0 & \text{if } p \text{ is unramified.} \end{cases}$$

Thus, when we count quartic D_4-extensions, the discriminant has the shape ab^2c^3.

Observations:

- main contribution comes from quadratic fields K with $D_K < \log\log\log\log X$;
- a positive proportion of the quartic D_4-extensions have a given quadratic field K as their subfield.

Difficulties with discriminant counting

Group theoretic properties greatly influence how difficult it is to count by discriminant, heavily exploited in previous works.

Difficulties with discriminant counting

Group theoretic properties greatly influence how difficult it is to count by discriminant, heavily exploited in previous works. Difficult example:

Example ($L/\mathbb{Q}$ Galois with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2^n}$)

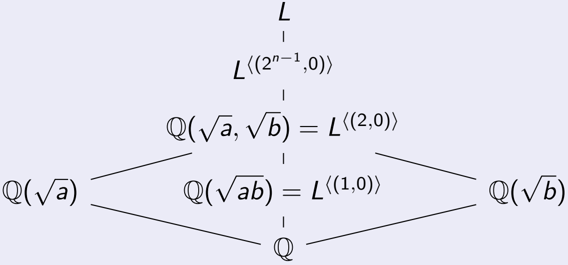
Note that $D_{2^n} = \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. *The elements of minimal order are* $(k, 1)$ *(reflections) and* $(2^{n-1}k, 0)$ *(rotations with order dividing* 2*).*

Difficulties with discriminant counting

Group theoretic properties greatly influence how difficult it is to count by discriminant, heavily exploited in previous works. Difficult example:

Example ($L/\mathbb{Q}$ Galois with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2^n}$)

Note that $D_{2^n} = \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. The elements of minimal order are $(k, 1)$ (reflections) and $(2^{n-1}k, 0)$ (rotations with order dividing 2).

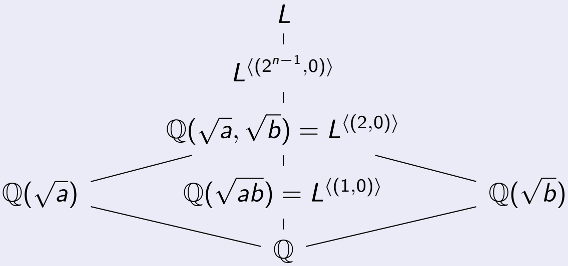


Difficulties with discriminant counting

Group theoretic properties greatly influence how difficult it is to count by discriminant, heavily exploited in previous works. Difficult example:

Example ($L/\mathbb{Q}$ Galois with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2^n}$)

Note that $D_{2^n} = \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. The elements of minimal order are $(k, 1)$ (reflections) and $(2^{n-1}k, 0)$ (rotations with order dividing 2).



Positive proportion of extensions have $L^{\langle(2^{n-1},0)\rangle}/\mathbb{Q}(\sqrt{ab})$ unramified. So at least as hard as getting distribution of $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$.

Fair counting functions

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Fair counting functions

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of “fair counting functions”.

Fair counting functions

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of “fair counting functions”.

Important examples of fair counting functions are the conductor and the product of ramified primes.

Fair counting functions

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of “fair counting functions”.

Important examples of fair counting functions are the conductor and the product of ramified primes.

Mäki (1993): Malle’s conjecture for abelian extensions ordered by conductor.

Fair counting functions

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of "fair counting functions".

Important examples of fair counting functions are the conductor and the product of ramified primes.

Mäki (1993): Malle's conjecture for abelian extensions ordered by conductor.

Wood (2010): Malle's conjecture for abelian extensions ordered by any fair counting function with local conditions.

Fair counting functions

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of "fair counting functions".

Important examples of fair counting functions are the conductor and the product of ramified primes.

Mäki (1993): Malle's conjecture for abelian extensions ordered by conductor.

Wood (2010): Malle's conjecture for abelian extensions ordered by any fair counting function with local conditions.

Altug–Shankar–Varma–Wilson (2017): Malle's conjecture for D_4 by Artin conductor.

Main result

A group G is called *nilpotent* if it is a direct product of p-groups.

Main result

A group G is called *nilpotent* if it is a direct product of p-groups.

Theorem (K.–Pagano)

Assume GRH. Let G be a nilpotent group with $\#G$ odd. Then

$$\liminf_{X \to \infty} \frac{\# \left\{ K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G \right\}}{c'(G) X (\log X)^{b'(G)}} \geq 1,$$

where $c'(G)$ is the expected Euler product and where $b'(G)$ is the naïve analogue of Malle's $b(G)$ in this situation.

Main result

A group G is called *nilpotent* if it is a direct product of p-groups.

Theorem (K.–Pagano)

Assume GRH. Let G be a nilpotent group with $\#G$ odd. Then

$$\liminf_{X \to \infty} \frac{\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\right\}}{c'(G) X (\log X)^{b'(G)}} \geq 1,$$

where $c'(G)$ is the expected Euler product and where $b'(G)$ is the naïve analogue of Malle's $b(G)$ in this situation.

Surprisingly, the corresponding asymptotic

$$\lim_{X \to \infty} \frac{\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\right\}}{c'(G) X (\log X)^{b'(G)}} = 1$$

is not true in general. Counterexamples exist for nilpotency class 2.

Inverse Galois problem

The assumption that $|G|$ is odd corresponds to the substantial difference in our understanding of the inverse Galois problem.

Inverse Galois problem

The assumption that $|G|$ is odd corresponds to the substantial difference in our understanding of the inverse Galois problem.

If $|G|$ is odd and nilpotent, the inverse Galois problem was solved by Scholz–Reichardt.

Inverse Galois problem

The assumption that $|G|$ is odd corresponds to the substantial difference in our understanding of the inverse Galois problem.

If $|G|$ is odd and nilpotent, the inverse Galois problem was solved by Scholz–Reichardt.

For 2-groups, the situation is much more involved. The only known proof is a famous result of Shafarevich (inverse Galois for solvable groups).

Scholz–Reichardt sketch I

Every nilpotent group can be built up from repeated central extensions, so we argue inductively.

Scholz–Reichardt sketch I

Every nilpotent group can be built up from repeated central extensions, so we argue inductively.

Let H be a p-group and let G be a central $\mathbb{F}_p$-extension of H, i.e.

$$1 \to \mathbb{F}_p \to G \to H \to 1.$$

Scholz–Reichardt sketch I

Every nilpotent group can be built up from repeated central extensions, so we argue inductively.

Let H be a p-group and let G be a central $\mathbb{F}_p$-extension of H, i.e.

$$1 \to \mathbb{F}_p \to G \to H \to 1.$$

Suppose that we have a H-extension $\pi : G_{\mathbb{Q}} \to H$, and consider

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{F}_p & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\ & & & & \uparrow{\scriptstyle ?} & \nearrow_{\pi} & & & \\ & & & & G_{\mathbb{Q}} & & & & \end{array}$$

Scholz–Reichardt sketch I

Every nilpotent group can be built up from repeated central extensions, so we argue inductively.

Let H be a p-group and let G be a central $\mathbb{F}_p$-extension of H, i.e.

$$1 \to \mathbb{F}_p \to G \to H \to 1.$$

Suppose that we have a H-extension $\pi : G_{\mathbb{Q}} \to H$, and consider

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{F}_p & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\ & & & & \uparrow {\scriptstyle ?} & \nearrow_{\pi} & & & \\ & & & & G_{\mathbb{Q}} & & & & \end{array}$$

It is well-known that we have a local-to-global for the above diagram, which roughly means that we have to control $\pi(\mathrm{Frob}_v)$ for all v.

Scholz–Reichardt sketch II

Note that H also fits in an exact sequence

$$1 \to \mathbb{F}_p \to H \to H' \to 1.$$

Therefore we may twist our H-extension $\pi : G_{\mathbb{Q}} \to H$ by $\chi : G_{\mathbb{Q}} \to \mathbb{F}_p$ to get $\pi + \chi : G_{\mathbb{Q}} \to H$.

Scholz–Reichardt sketch II

Note that H also fits in an exact sequence

$$1 \to \mathbb{F}_p \to H \to H' \to 1.$$

Therefore we may twist our H-extension $\pi : G_{\mathbb{Q}} \to H$ by $\chi : G_{\mathbb{Q}} \to \mathbb{F}_p$ to get $\pi + \chi : G_{\mathbb{Q}} \to H$.

Idea: we take χ_ℓ to be of prime conductor ℓ, unramified in π, and use it to fix the Frobenius elements at all primes ramified in π.

Scholz–Reichardt sketch II

Note that H also fits in an exact sequence

$$1 \to \mathbb{F}_p \to H \to H' \to 1.$$

Therefore we may twist our H-extension $\pi : G_{\mathbb{Q}} \to H$ by $\chi : G_{\mathbb{Q}} \to \mathbb{F}_p$ to get $\pi + \chi : G_{\mathbb{Q}} \to H$.

Idea: we take χ_ℓ to be of prime conductor ℓ, unramified in π, and use it to fix the Frobenius elements at all primes ramified in π.

The resulting map $\pi + \chi_\ell : G_{\mathbb{Q}} \to \mathbb{F}_p$ also ramifies at ℓ, so we need to check local-to-global also at ℓ.

Scholz–Reichardt sketch II

Note that H also fits in an exact sequence

$$1 \to \mathbb{F}_p \to H \to H' \to 1.$$

Therefore we may twist our H-extension $\pi : G_{\mathbb{Q}} \to H$ by $\chi : G_{\mathbb{Q}} \to \mathbb{F}_p$ to get $\pi + \chi : G_{\mathbb{Q}} \to H$.

Idea: we take χ_ℓ to be of prime conductor ℓ, unramified in π, and use it to fix the Frobenius elements at all primes ramified in π.

The resulting map $\pi + \chi_\ell : G_{\mathbb{Q}} \to \mathbb{F}_p$ also ramifies at ℓ, so we need to check local-to-global also at ℓ.

Here we use that p is odd in an essential way: $\chi_\ell(\mathrm{Frob}_q)$ and $\chi_q(\mathrm{Frob}_\ell)$ are independent.

Step 1a: parametrization

To give an idea how the techniques work, we will (unconditionally!) give an overview for the proof of the asymptotic for the number of Galois D_4-extensions by product of ramified primes.

Step 1a: parametrization

To give an idea how the techniques work, we will (unconditionally!) give an overview for the proof of the asymptotic for the number of Galois D_4-extensions by product of ramified primes.

We have a central exact sequence

$$0 \to \mathbb{F}_2 \to D_4 \xrightarrow{q} \mathbb{F}_2^2 \to 0$$

and a bijection

$$\mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2^2) \leftrightarrow \{(a, b) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 : a, b \text{ lin. ind.}\}.$$

Step 1a: parametrization

To give an idea how the techniques work, we will (unconditionally!) give an overview for the proof of the asymptotic for the number of Galois D_4-extensions by product of ramified primes.

We have a central exact sequence

$$0 \to \mathbb{F}_2 \to D_4 \xrightarrow{q} \mathbb{F}_2^2 \to 0$$

and a bijection

$$\mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2^2) \leftrightarrow \{(a, b) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 : a, b \text{ lin. ind.}\}.$$

Given $\pi \in \mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2^2)$, this leads to the *central embedding problem*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{F}_2 & \longrightarrow & D_4 & \longrightarrow & \mathbb{F}_2^2 & \longrightarrow & 0 \\ & & & & \uparrow ? & \nearrow \pi & & & \\ & & & & G_{\mathbb{Q}} & & & & \end{array}$$

Step 1a: parametrization

To give an idea how the techniques work, we will (unconditionally!) give an overview for the proof of the asymptotic for the number of Galois D_4-extensions by product of ramified primes.

We have a central exact sequence

$$0 \to \mathbb{F}_2 \to D_4 \xrightarrow{q} \mathbb{F}_2^2 \to 0$$

and a bijection

$$\mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2^2) \leftrightarrow \{(a, b) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^2 : a, b \text{ lin. ind.}\}.$$

Given $\pi \in \mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2^2)$, this leads to the *central embedding problem*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{F}_2 & \longrightarrow & D_4 & \longrightarrow & \mathbb{F}_2^2 & \longrightarrow & 0 \\ & & & & \uparrow ? & \nearrow_{\pi} & & & \\ & & & & G_{\mathbb{Q}} & & & & \end{array}$$

It is well-known that a $\mathbb{F}_2^2$-extension $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ of $\mathbb{Q}$ is contained in a D_4-extension if and only if $x^2 = ay^2 + bz^2$ has a non-trivial point.

Step 1b: parametrization

If $\rho \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4)$ is a lift of $\pi \in \mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2)$ and $q : D_4 \twoheadrightarrow \mathbb{F}_2^2$, then

$$\{f \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4) : f \circ q = \pi\} = \{\rho \cdot \chi : \chi \in \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{F}_2)\}.$$

Step 1b: parametrization

If $\rho \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4)$ is a lift of $\pi \in \mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2)$ and $q : D_4 \twoheadrightarrow \mathbb{F}_2^2$, then

$$\{f \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4) : f \circ q = \pi\} = \{\rho \cdot \chi : \chi \in \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{F}_2)\}.$$

Therefore we have a bijection

$$\mathrm{Epi}(G_{\mathbb{Q}}, D_4) \leftrightarrow \{(a, b, c) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 : a, b \text{ ind.}, x^2 = ay^2 + bz^2 \text{ sol.}\}.$$

Step 1b: parametrization

If $\rho \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4)$ is a lift of $\pi \in \mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2)$ and $q : D_4 \twoheadrightarrow \mathbb{F}_2^2$, then

$$\{f \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4) : f \circ q = \pi\} = \{\rho \cdot \chi : \chi \in \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{F}_2)\}.$$

Therefore we have a bijection

$$\mathrm{Epi}(G_{\mathbb{Q}}, D_4) \leftrightarrow \{(a, b, c) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 : a, b \text{ ind.}, x^2 = ay^2 + bz^2 \text{ sol.}\}.$$

Under this parametrization, the product of ramified primes maps to $\mathrm{rad}(|abc|)$ (ignoring minor issues with ramification at 2).

Step 1b: parametrization

If $\rho \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4)$ is a lift of $\pi \in \mathrm{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2)$ and $q : D_4 \twoheadrightarrow \mathbb{F}_2^2$, then

$$\{f \in \mathrm{Epi}(G_{\mathbb{Q}}, D_4) : f \circ q = \pi\} = \{\rho \cdot \chi : \chi \in \mathrm{Hom}(G_{\mathbb{Q}}, \mathbb{F}_2)\}.$$

Therefore we have a bijection

$$\mathrm{Epi}(G_{\mathbb{Q}}, D_4) \leftrightarrow \{(a, b, c) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 : a, b \text{ ind.}, x^2 = ay^2 + bz^2 \text{ sol.}\}.$$

Under this parametrization, the product of ramified primes maps to $\mathrm{rad}(|abc|)$ (ignoring minor issues with ramification at 2).

It turns out to be more convenient to work with seven variables α_S for $\emptyset \subset S \subseteq \{a, b, c\}$, where α_S is the product over all primes p dividing the variables in S and not dividing the variables in $\{a, b, c\} - S$.

Step 1b: parametrization

If $\rho \in \text{Epi}(G_{\mathbb{Q}}, D_4)$ is a lift of $\pi \in \text{Epi}(G_{\mathbb{Q}}, \mathbb{F}_2)$ and $q : D_4 \twoheadrightarrow \mathbb{F}_2^2$, then

$$\{f \in \text{Epi}(G_{\mathbb{Q}}, D_4) : f \circ q = \pi\} = \{\rho \cdot \chi : \chi \in \text{Hom}(G_{\mathbb{Q}}, \mathbb{F}_2)\}.$$

Therefore we have a bijection

$$\text{Epi}(G_{\mathbb{Q}}, D_4) \leftrightarrow \{(a, b, c) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 : a, b \text{ ind.}, x^2 = ay^2 + bz^2 \text{ sol.}\}.$$

Under this parametrization, the product of ramified primes maps to $\text{rad}(|abc|)$ (ignoring minor issues with ramification at 2).

It turns out to be more convenient to work with seven variables α_S for $\emptyset \subset S \subseteq \{a, b, c\}$, where α_S is the product over all primes p dividing the variables in S and not dividing the variables in $\{a, b, c\} - S$.

The variables α_S are squarefree and pairwise coprime, and we have $\text{rad}(|abc|) = \prod_{\emptyset \subset S \subseteq \{a,b,c\}} |\alpha_S|$.

Step 2: character sums

Define $T(a)$ to be the subsets of $\{a, b, c\}$ containing a. Then we have

$$a = \prod_{S \in T(a)} \alpha_S$$

and similarly for b, c.

Step 2: character sums

Define $T(a)$ to be the subsets of $\{a, b, c\}$ containing a. Then we have

$$a = \prod_{S \in T(a)} \alpha_S$$

and similarly for b, c. So to count D_4-extensions, must evaluate

$$\sum_{\substack{\prod_{\emptyset \subset S \subseteq \{a,b,c\}} |\alpha_S| \leq X \\ a,b \text{ lin. ind.}}} \mu^2\left(\prod_S |\alpha_S|\right) \cdot \mathbf{1}_{x^2 = \alpha_a \alpha_{a,b} \alpha_{a,c} \alpha_{a,b,c} y^2 + \alpha_b \alpha_{a,b} \alpha_{b,c} \alpha_{a,b,c} z^2 \text{ sol.}} \cdot$$

Step 2: character sums

Define $T(a)$ to be the subsets of $\{a, b, c\}$ containing a. Then we have

$$a = \prod_{S \in T(a)} \alpha_S$$

and similarly for b, c. So to count D_4-extensions, must evaluate

$$\sum_{\substack{\prod_{\emptyset \subset S \subseteq \{a,b,c\}} |\alpha_S| \leq X \\ a,b \text{ lin. ind.}}} \mu^2 \left(\prod_S |\alpha_S| \right) \cdot \mathbf{1}_{x^2 = \alpha_a \alpha_{a,b} \alpha_{a,c} \alpha_{a,b,c} y^2 + \alpha_b \alpha_{a,b} \alpha_{b,c} \alpha_{a,b,c} z^2 \text{ sol.}} \cdot$$

Hasse-Minkowski: detect solubility of conic locally at primes dividing α_S.

Step 2: character sums

Define $T(a)$ to be the subsets of $\{a, b, c\}$ containing a. Then we have

$$a = \prod_{S \in T(a)} \alpha_S$$

and similarly for b, c. So to count D_4-extensions, must evaluate

$$\sum_{\substack{\prod_{\emptyset \subset S \subseteq \{a,b,c\}} |\alpha_S| \leq X \\ a,b \text{ lin. ind.}}} \mu^2 \left(\prod_S |\alpha_S| \right) \cdot \mathbf{1}_{x^2 = \alpha_a \alpha_{a,b} \alpha_{a,c} \alpha_{a,b,c} y^2 + \alpha_b \alpha_{a,b} \alpha_{b,c} \alpha_{a,b,c} z^2 \text{ sol.}} \cdot$$

Hasse-Minkowski: detect solubility of conic locally at primes dividing α_S.

Now rewrite the above sum as a sum over Legendre symbols involving the variables α_S.

Step 3: equidistribution

Evaluate the resulting character sum using Chebotarev and the large sieve.

Step 3: equidistribution

Evaluate the resulting character sum using Chebotarev and the large sieve.

How does this process generalize?

Step 3: equidistribution

Evaluate the resulting character sum using Chebotarev and the large sieve.

How does this process generalize?

- Build a nilpotent extension by iterated central extensions. This yields a parametrization of G-extensions by tuples of squarefree integers satisfying central embedding problems.

Step 3: equidistribution

Evaluate the resulting character sum using Chebotarev and the large sieve.

How does this process generalize?

- Build a nilpotent extension by iterated central extensions. This yields a parametrization of G-extensions by tuples of squarefree integers satisfying central embedding problems.
- These central embedding problems get much more complicated, but still satisfy local-to-global and are certainly determined by Frob_p for p dividing the variables of the parametrization.

Step 3: equidistribution

Evaluate the resulting character sum using Chebotarev and the large sieve.

How does this process generalize?

- Build a nilpotent extension by iterated central extensions. This yields a parametrization of G-extensions by tuples of squarefree integers satisfying central embedding problems.
- These central embedding problems get much more complicated, but still satisfy local-to-global and are certainly determined by Frob_p for p dividing the variables of the parametrization.
- In our chosen ordering, a typical extension is a rather large twist of a "minimally ramified central extension". Getting equidistribution of Frobenius in minimally ramified extensions is *very hard*. The key idea of the proof is to exploit the twisting.

Step 3: equidistribution

Evaluate the resulting character sum using Chebotarev and the large sieve.

How does this process generalize?

- Build a nilpotent extension by iterated central extensions. This yields a parametrization of G-extensions by tuples of squarefree integers satisfying central embedding problems.
- These central embedding problems get much more complicated, but still satisfy local-to-global and are certainly determined by Frob_p for p dividing the variables of the parametrization.
- In our chosen ordering, a typical extension is a rather large twist of a "minimally ramified central extension". Getting equidistribution of Frobenius in minimally ramified extensions is *very hard*. The key idea of the proof is to exploit the twisting.
- Proof can most likely be made unconditional with a suitably strong large sieve for nilpotent extensions.

Arithmetic Statistics

I would like to thank the organizers Elisa, Jan, Peter and Samuele for a wonderful conference.

I would like to thank the organizers Elisa, Jan, Peter and Samuele for a wonderful conference.

Happy birthday Peter!