COMPOSITIO MATHEMATICA

Non-abelian Cohen–Lenstra heuristics over function fields

Nigel Boston and Melanie Matchett Wood

Compositio Math. **153** (2017), 1372–1390.

doi:10.1112/S0010437X17007102

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
EST. 1865

Compositio Math. 153 (2017) 1372–1390
doi:10.1112/S0010437X17007102

Non-abelian Cohen–Lenstra heuristics over function fields

Nigel Boston and Melanie Matchett Wood

Abstract

Boston, Bush and Hajir have developed heuristics, extending the Cohen–Lenstra heuristics, that conjecture the distribution of the Galois groups of the maximal unramified pro-p extensions of imaginary quadratic number fields for p an odd prime. In this paper, we find the moments of their proposed distribution, and further prove there is a unique distribution with those moments. Further, we show that in the function field analog, for imaginary quadratic extensions of $\mathbb{F}_q(t)$, the Galois groups of the maximal unramified pro-p extensions, as $q \to \infty$, have the moments predicted by the Boston, Bush and Hajir heuristics. In fact, we determine the moments of the Galois groups of the maximal unramified pro-odd extensions of imaginary quadratic function fields, leading to a conjecture on Galois groups of the maximal unramified pro-odd extensions of imaginary quadratic number fields.

1. Introduction

We fix an odd prime p throughout the paper. The Cohen–Lenstra heuristics [CL84] predict the distribution of abelian p-groups that show up as the p-primary part of the class group of an imaginary quadratic number field as we vary the field. In particular, there is a measure μ_{CL} on finite abelian p-groups, such that $\mu_{\mathrm{CL}}(G) > 0$ for every finite abelian p-group G, that is uniquely characterized by the fact that for any G_1, G_2 finite abelian p-groups $\mu_{\mathrm{CL}}(G_1)/\mu_{\mathrm{CL}}(G_2) = |\mathrm{Aut}(G_2)|/|\mathrm{Aut}(G_1)|$. We let D_X denote the set of imaginary quadratic fields of absolute discriminant less than X, and let C_K denote the p-primary part of the class group of a field K, called the p-class group of K. Cohen and Lenstra then conjecture the following.

Conjecture 1.1 (Cohen–Lenstra, [CL84, 8.1]). For any 'reasonable' function f on isomorphism classes of finite abelian p-groups, we have

$$\lim_{X\to\infty} \frac{\sum_{K\in D_X} f(C_K)}{\#D_X} = \int_G f(G)\, d\mu_{\mathrm{CL}}.$$

By class field theory, the p-class group of a number field K is isomorphic to the Galois group A_K of the maximal abelian unramified p-extension of K. We use this perspective in which Cohen–Lenstra predicts the distribution of Galois groups of such extensions to consider a generalization of the above conjecture to non-abelian unramified extensions of imaginary quadratic fields K, as follows.

Received 12 April 2016, accepted in final form 12 January 2017, published online 12 May 2017.
2010 Mathematics Subject Classification 11G20, 11R11, 11R29, 11R58, 11R45 (primary).
Keywords: Cohen–Lenstra heuristics, p-class tower groups, unramified extensions, quadratic fields.

Let G_K be the Galois group of the maximal unramified pro-p extension of K, also called its *p-class tower group*. Boston *et al.* [BBH16] have made predictions about how often one should expect a given group to appear as G_K. Unlike A_K, it turns out that G_K can be infinite and this introduces new features in the non-abelian case, for example, the measure on candidate groups is no longer discrete. We put a measure μ_{BBH} on the set of finitely generated pro-p groups (see § 3 for the precise definition), so that the conjecture of Boston, Bush and Hajir is the following.

Conjecture 1.2 (Boston–Bush–Hajir, cf. [BBH16]). For any 'reasonable' function f on isomorphism classes of pro-p groups, we have

$$\lim_{X\to\infty} \frac{\sum_{K\in D_X} f(G_K)}{\# D_X} = \int_G f(G)\, d\mu_{\mathrm{BBH}}.$$

Of such reasonable f, certain are particularly interesting, and their averages $\int_G f(G)\, d\mu_{\mathrm{BBH}}$ we call the *moments* of the measure μ_{BBH}. To define these f, first note that the p-class tower group G_K has a generator-inverting automorphism σ coming from the action of $\mathrm{Gal}(K/\mathbb{Q})$. If G and H are both profinite groups for which we have a chosen automorphism (we call both automorphisms σ), then we write $\mathrm{Sur}_\sigma(G,H)$ for the continuous 'σ-equivariant' surjections from G to H. The measure μ_{BBH} is supported on groups G with a unique, up to conjugation, generator-inverting automorphism, which we also denote as σ. The average $\int_G |\mathrm{Sur}_\sigma(G,H)|\, d\mu_{\mathrm{BBH}}$ is called the *H-moment* of the measure $d\mu_{\mathrm{BBH}}$, and we determine these moments. (See § 7 for the simple relationship between these moments and the analog without the σ-equivariant condition.)

Theorem 1.3 (Moments of μ_{BBH}). *For every finite p-group H with a generator-inverting automorphism σ, we have*

$$\int_G |\mathrm{Sur}_\sigma(G,H)|\, d\mu_{\mathrm{BBH}} = 1. \tag{1}$$

Theorem 1.3 will be proven as part of Theorem 4.1 below. Further, we show that these moments characterize the measure $d\mu_{\mathrm{BBH}}$.

Theorem 1.4 (Moments characterize μ_{BBH}). *If ν is a measure (for the σ-algebra Ω generated by groups with a fixed p-class c quotient; these terms will be defined in § 3) on the set of isomorphism classes of finitely generated pro-p groups such that*

$$\int_G |\mathrm{Sur}_\sigma(G,H)|\, d\nu = 1$$

for every finite p-group H with a generator-inverting automorphism σ, then $\nu = \mu_{\mathrm{BBH}}$.

In fact, in Theorem 4.9 we prove a slightly stronger version of Theorem 1.4 in which we only use some of the moments. If we take H in (1) to be abelian and note that under abelianization μ_{BBH} pushes forward to μ_{CL}, then we recover the observation of Ellenberg *et al.* [EVW16, § 8.1] that the A-moments of μ_{CL} are 1 for every abelian p-group A. They have also shown that these A-moments characterize μ_{CL} [EVW16, Lemma 8.2]. The collection of moments given by averaging $|\mathrm{Sur}_\sigma(-,H)|$ is a fixed upper triangular transformation from the averages of $|\mathrm{Hom}_\sigma(-,H)|$. For finite abelian groups, these latter averages are the mixed moments (of the standard invariants of the group) in the usual sense (see [CKLPW15, § 3.3]).

In this paper, we prove a theorem towards the function field analog of Conjecture 1.2. We consider the function field $\mathbb{F}_q(t)$, where q is a prime power. We say $K/\mathbb{F}_q(t)$ is *imaginary quadratic* if K is a degree-2 extension of $\mathbb{F}_q(t)$ that is ramified at the place corresponding to $1/t$, or equivalently, the smooth, projective hyperelliptic curve corresponding to K is ramified over ∞. For a quadratic extension $K/\mathbb{F}_q(t)$, we let $K^{\mathrm{un},\infty}$ be the maximal unramified extension of K that is split completely over every place of K that lies over the place ∞ in $\mathbb{F}_q(t)$, and let $G_K^{\mathrm{un},\infty} = \mathrm{Gal}(K^{\mathrm{un},\infty}/K)$, with a generator-inverting automorphism σ coming from the action of $\mathrm{Gal}(K/\mathbb{F}_q(t))$ (see § 2).

Theorem 1.5. *Let H be a finite odd-order group with a generator-inverting automorphism such that the center of H contains no elements fixed by σ except the identity. Let*

$$\delta_q^+ := \limsup_{m\to\infty} \frac{\sum_{K\in E_m} |\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|}{\# E_m} \quad \text{and} \quad \delta_q^- := \liminf_{m\to\infty} \frac{\sum_{K\in E_m} |\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|}{\# E_m},$$

where E_m denotes the set of imaginary quadratic extensions $\mathbb{F}_q(t)$ with discriminant of norm q^{2m+2}. Then as $q \to \infty$ among prime powers relatively prime to $2|H|$ and with $(q-1, |H|) = 1$, we have

$$\delta_q^+, \quad \delta_q^- \to 1.$$

In light of Theorems 1.3 and 1.4, this is good evidence for Conjecture 1.2. When H is a p-group, the surjections in Theorem 1.5 factor through the maximal pro-p quotient of $G_K^{\mathrm{un},\infty}$, which is analogous to the G_K defined above. If we have an analogy between $\mathbb{F}_q(t)$ and $\mathbb{Q}$ for any q, then the q limits in Theorem 1.5 should not matter, and after that limit we get agreement with the μ_{BBH} moments by Theorem 1.3. Since these moments determine a unique measure by Theorem 1.4, that suggests Conjecture 1.2 for general f, though technically the G_K do not have to be distributed according to a measure, but only a limit of measures.

Further, if we assume a vanishing conjecture on the homology of Hurwitz spaces, then under the hypotheses of Theorem 1.5 we would in fact obtain that for $q \geqslant N(H)$ we have $\delta_q^+ = \delta_q^- = 1$ (see Theorem 6.6). Theorem 1.5 suggests the following conjecture, extending Conjecture 1.2 from pro-p groups to pro-odd groups, at least in the case of the moments.

Conjecture 1.6. For any imaginary quadratic number field K, let $\mathcal{G}_K$ be the maximal pro-odd quotient of the Galois group of the maximal unramified extension of K. Then for every finite odd group H with a generating-inverting automorphism

$$\lim_{X\to\infty} \frac{\sum_{K\in D_X} \mathrm{Sur}_\sigma(\mathcal{G}_K, H)}{\# D_X} = 1.$$

Bhargava [Bha14, § 1.2] has asked what we should expect for the average number of H quotients of $G_K^{\mathrm{un},\infty}$, for any H. Conjecture 1.6 suggests the answer for odd H. (See § 7 for the translation from our conjecture for σ-equivariant quotients to the consequence for more general quotients.) Bhargava [Bha14, § 1.2] has proven some intriguing moments for $H = A_3, A_4, A_5, S_3, S_4, S_5$.

It would be interesting to have a concrete description of an underlying measure on pro-odd groups that gives the moments on Conjecture 1.6, as μ_{BBH} does in the pro-p case. However, before making a conjectural analog of Conjecture 1.2, one should note it is an open question whether $\mathcal{G}_K$ is (topologically) finitely generated or not, let alone finitely presented.

In order to prove Theorem 1.5, in § 5, we translate the sum of counts of surjections to a count of extensions of $\mathbb{F}_q(t)$ with certain properties. We then, in § 6, apply the recent powerful results of Ellenberg *et al.* [EVW16, EVW12] on homological stability of Hurwitz spaces and the components of Hurwitz spaces along with their Galois action over $\mathbb{F}_q$ in order to count the extensions. A main motivation for the work of Ellenberg, Venkatesh and Westerland is to prove function field analogs of Conjecture 1.1. In particular, [EVW16, Theorem 8.8] gives the case of Theorem 1.5 when H is an abelian p-group. The analysis of components of Hurwitz spaces in [EVW12] gives the number of components in terms of certain group-theoretically defined quantities, which we compute in the cases necessary for our application. We apply results on Hurwitz spaces from [EVW16, EVW12], the Grothendieck–Lefschetz trace formula, and our group theory computation to count $\mathbb{F}_q$ points of a moduli space that parametrize the relevant extensions of $\mathbb{F}_q(t)$.

Finally, we make some remarks on the hypotheses in Theorem 1.5. The condition on the center of H comes from a technical limitation of [EVW12]. The requirement that $(q-1,|H|)=1$ ensures that the base field does not have 'extra roots of unity.' The case of extra roots of unity is one in which even the Cohen–Lenstra heuristics are expected to be wrong [Mal08] and new heuristics have been proposed by Garton [Gar15] and Adam and Malle [AM15] for that case. To the authors' knowledge, there is no work on even the Cohen–Lenstra heuristics in the function field setting when $(q,|H|)>1$ or $2\mid q$.

2. Background on non-abelian analogs of class groups

Let Q be a global field and ∞ a place of Q. In this paper, we are interested in the cases $Q=\mathbb{Q}$ or $\mathbb{F}_q(t)$ with the usual infinite place. For a separable, quadratic extension K/Q, we let $K^{\mathrm{un},\infty}$ be the maximal unramified extension of K that is split completely over all places of K over ∞, and let $G_K^{\mathrm{un},\infty}=\mathrm{Gal}(K^{\mathrm{un},\infty}/K)$. We let G_K be the maximal pro-p quotient of $G_K^{\mathrm{un},\infty}$.

Remark 2.1. While it looks like we have added the condition at ∞ compared with the definition of G_K for number fields in the introduction, we could in fact add this condition to the definition of G_K for a quadratic number field K without effect because, for an archimedean place, unramified is the same as split completely. Also, if $Q=\mathbb{F}_q(t)$ and $\mathcal{O}_K$ is the integral closure of $\mathbb{F}_q[t]$ in K, then class field theory gives that the abelianization $(G_K^{\mathrm{un},\infty})^{\mathrm{ab}}$ is isomorphic to the class group $Cl(\mathcal{O}_K)$ of ideals modulo principal ideals, so $G_K^{\mathrm{un},\infty}$ is the natural function field analog of a 'non-abelian class group'.

Lemma 2.2. *If K/Q is a separable, quadratic extension, then all inertia subgroups of* $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$ *and the decomposition group at infinity are contained in*

$$\{1\}\cup\{r\in\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)\backslash G_K^{\mathrm{un},\infty}\mid r^2=1\}.$$

Proof. The intersection with $G_K^{\mathrm{un},\infty}$ of any inertia subgroup or the decomposition group at infinity is trivial by the definition of $K^{\mathrm{un},\infty}$, which also implies they have order at most 2. □

If Q is a global field and ∞ is a place of Q such that Q has no non-trivial finite extensions unramified everywhere and split completely over ∞ (such as in our cases of interest $Q=\mathbb{Q}$ or $\mathbb{F}_q(t)$), we call Q,∞ *rational-like*. Then we have that $\{r\in\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)\backslash G_K^{\mathrm{un},\infty}\mid r^2=1\}$ is non-empty. So the exact sequence

$$1\to G_K^{\mathrm{un},\infty}\to\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)\to\mathrm{Gal}(K/Q)\to 1$$

splits. Any lift of the generator of $\mathrm{Gal}(K/Q)$ gives an order-2 automorphism of $G_K^{\mathrm{un},\infty}$ by conjugation.

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

Proposition 2.3. *Let Q, ∞ be rational-like and K/Q a separable, quadratic extension. The action of an element $\tau \in \mathrm{Gal}(K^{\mathrm{un},\infty}/Q) \backslash G_K^{\mathrm{un},\infty}$ of order 2 on $G_K^{\mathrm{un},\infty}$ by conjugation inverts a set of (topological) generators of $G_K^{\mathrm{un},\infty}$.*

Proof. We write $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q) = G_K^{\mathrm{un},\infty} \rtimes \langle\tau\rangle$. Let R be the closed subgroup of $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$ generated by $\{r \in \mathrm{Gal}(K^{\mathrm{un},\infty}/Q) \backslash G_K^{\mathrm{un},\infty} \mid r^2 = 1\}$. From the definition, it follows that R is normal. So R corresponds to a subfield M of $K^{\mathrm{un},\infty}$, which is Galois over Q, and such that in $\mathrm{Gal}(M/Q)$ all inertia groups are trivial and the decomposition group at infinity is trivial by Lemma 2.2. It follows that $M = Q$. The order-2 elements of $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q) \backslash G_K^{\mathrm{un},\infty}$ are the (g_i, τ), for $g_i \in G_K^{\mathrm{un},\infty}$ such that $g_i^\tau = g_i^{-1}$. So the words in $\{(g_i, \tau) \mid g_i \in G_K^{\mathrm{un},\infty}, g_i^\tau = g_i^{-1}\}$ are dense in $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$. An element of $G_K^{\mathrm{un},\infty}$ equivalent to one of these words is a word in the symbols $\{g_i \in G_K^{\mathrm{un},\infty} \mid g_i^\tau = g_i^{-1}\}$, and such elements are a dense subgroup of $G_K^{\mathrm{un},\infty}$. Thus the set $\{g_i \in G_K^{\mathrm{un},\infty} \mid g_i^\tau = g_i^{-1}\}$ topologically generates $G_K^{\mathrm{un},\infty}$. □

In light of Proposition 2.3, we pick a lift τ of the generator of $\mathrm{Gal}(K/Q)$ to $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$ and let conjugation by τ be our chosen generator-inverting automorphism σ of $G_K^{\mathrm{un},\infty}$. Further, the Schur–Zassenhaus theorem [Wil98, Proposition 2.3.3] guarantees that all the lifts of the generator of $\mathrm{Gal}(K/Q)$ to the pro-p quotient G_K of $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$ (or the pro-odd quotient) are conjugate. Thus for an odd finite group H with automorphism σ, we then have that $|\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|$ does not depend on the choice of τ.

3. Boston–Bush–Hajir heuristics: background and notation

Koch and Venkov [KV75] have shown that for an imaginary quadratic extension $K/\mathbb{Q}$, the group G_K satisfies certain properties we will now outline. For a pro-p group G, let $d(G) := \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $r(G) := \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G, \mathbb{Z}/p\mathbb{Z})$. These are, respectively, the generator rank and the relation rank of G as a pro-p group. For a pro-finite group G, we define a *GI-automorphism* of G to be a $\sigma \in \mathrm{Aut}(G)$ such that σ acts as inversion on a set of (topological) generators. For a pro-p group, this is equivalent to requiring that $\sigma^2 = 1$, which σ are called *involutions*, and σ acts as inversion on the abelianization of G [Bos91].

Definition. A *Schur-σ* group is a finitely generated pro-p group G with finite abelianization such that:

(a) $d(G) = r(G)$ (then called just the *rank* of G);

(b) G admits a GI-automorphism.

Koch and Venkov [KV75] have shown that for an imaginary quadratic extension $K/\mathbb{Q}$, the group G_K is a Schur-σ group. The groups G_K we are considering in the function field case are also Schur-σ groups when $p \nmid q - 1$. This follows by class field theory, Proposition 2.3 above, and the upper bound on $r(G_K) - d(G_K)$, namely 0, due to Shafarevich, given as [HM01, Theorem 2.2]. Note that $r(G_K) - d(G_K) \geqslant 0$ since G_K^{ab} is finite and so the upper bound of 0 yields $r(G_K) - d(G_K) = 0$.

We will put a measure on the set of isomorphism classes of Schur σ-groups in order to state the Boston–Bush–Hajir heuristics. For this, we first need to define a σ-algebra (in the sense of measure theory – not our automorphism σ) on this set. Since many infinite Schur σ-groups are expected to occur as G_K with density 0, it makes sense to focus on certain finite quotients of these groups.

Any pro-p group G has a *lower p-central series* defined as $P_0(G) := G$ and for $n \geqslant 0$, we let $P_{n+1}(G)$ be the closed subgroup generated by $[G, P_n(G)]$ and $P_n(G)^p$. The groups $P_0(G) \geqslant P_1(G) \geqslant P_2(G) \geqslant \cdots$ form a descending chain of characteristic subgroups of G called the lower

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

p-central series. The p-*class* of a finite p-group G is the smallest $c \geqslant 0$ for which $P_c(G) = \{1\}$. Note that for a finitely generated pro-p group G, the successive quotients $P_n(G)/P_{n+1}(G)$ are finite abelian groups of exponent p, and so, in particular, if $P_c(G) = \{1\}$, then G must be finite. The lower p-central series and p-class can be thought of as analogous to the lower central series and nilpotency class, respectively. Note that $P_1(G)$ is also the Frattini subgroup $\Phi(G)$.

For a pro-p group G, we define $Q_c(G) := G/P_c(G)$, the maximal quotient of G with p-class at most c. So $Q_c(G_K)$ is the Galois group of the maximal unramified p-extension of K among extensions of Galois group with p-class at most c. Note that since a Schur σ-group G (such as G_K) is finitely generated, we have that $Q_c(G)$ is finite. It may be that $Q_c(G)$ has p-class strictly less than c: certainly when G itself has p-class strictly less than c, this happens, but in fact since the subquotients of the lower p-central series for G and for $Q_c(G)$ are the same up to index c, this is the only way it can happen.

Let Ω be the σ-algebra on the set of isomorphism classes of Schur σ-groups generated by the sets

$$\{G \mid Q_c(G) \simeq P\} \tag{2}$$

for each finite p-group P and fixed c. For example, we can fix a Schur σ-group G_0 and take the intersection over all c of $\{G \mid Q_c(G) \simeq Q_c(G_0)\}$ to see that Ω contains the singleton set containing the class of G_0.

We will next define a measure on the set of isomorphism classes of Schur σ-groups for a σ-algebra containing Ω. Any Schur σ-group of rank g can be presented as a quotient of the free pro-p group F_g on g generators $x_1, \ldots, x_g$ (with GI-automorphism $\sigma(x_i) = x_i^{-1}$) by g relations chosen from $X = \{s \in \Phi(F_g) \mid \sigma(s) = s^{-1}\}$. Since X is a closed subset of the profinite group F_g, we have a natural profinite probability measure μ on X from the limit of the uniform measures on finite quotients of F_g, on the σ-algebra generated by fibers of these quotients.

The Boston–Bush–Hajir probability measure μ_{BBH} will be given by randomly selecting such relations. However, this only gives a measure for a fixed rank g of Schur σ-groups. Since, however, the rank of a Schur σ-group is the rank of its abelianization (in fact, of the quotient of the abelianization $G/\Phi(G)$, by the Burnside basis theorem), we can use the Cohen–Lenstra heuristics to predict how often each rank g occurs. Let

$$\mu_{\mathrm{CL}}(g) := \sum_{G \text{ fin. ab., rk } g \text{ } p\text{-gp}} \mu_{\mathrm{CL}}(G) = p^{-g^2} \prod_{k=1}^{g} (1 - p^{-k})^{-2} \prod_{i=1}^{\infty} (1 - p^{-i}).$$

The above formula is from [CL84, Theorem 6.3]. Let A be a set of isomorphism classes of rank g Schur σ-groups. Then we define

$$\mu_{\mathrm{BBH}}(A) := \mu_{\mathrm{CL}}(g)\mu(\{(r_1, \ldots, r_g) \in X^g \mid F_g/\langle\langle r_1, \ldots, r_g \rangle\rangle \in A\}),$$

whenever $\{(r_1, \ldots, r_g) \in X^g \mid F_g/\langle\langle r_1, \ldots, r_g \rangle\rangle \in A\}$ is measurable, where the double angle brackets denote the closed normal subgroup generated by the elements. We can think of this measure as generating a random group by picking a rank g according to the Cohen–Lenstra measure and then independently creating a random Schur σ-group of rank g by taking the quotient of the free pro-p group F_g on g generators by g randomly chosen relations in X. Note that this process does not necessarily produce a Schur σ-group, as there may be redundancy among the relations and so the resulting group may not have relation rank g. However, such redundancy happens with probability 0 (the abelianization would be infinite, and, as noted by Friedman and Washington [FW89], this occurs with zero probability under μ_{CL}, which is induced on abelianizations from μ_{BBH} [BBH16, Theorem 2.20]).

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

Let $X_c = \{s \in \Phi(Q_c(F_g)) \mid \sigma(s) = s^{-1}\}$. Note that X_c is a finite set and has a uniform discrete probability measure μ_c that pulls back to μ on X. If P is a fixed finite p-group with $d(P) = g$, we define $\mu_{\mathrm{BBH},c}(P) := \mu_{\mathrm{BBH}}(\{G \mid Q_c(G) \simeq P\})$, and then

$$\mu_{\mathrm{BBH},c}(P) = \mu_{\mathrm{CL}}(g)\mu_c(\{(r_1,\ldots,r_g) \in X_c^g \mid Q_c(F_g)/\langle\langle r_1,\ldots,r_g\rangle\rangle \simeq P\}).$$

In particular $\{G \mid Q_c(G) \simeq P\}$ is measurable for μ_{BBH}.

If $P \simeq Q_c(G)$ for some Schur σ-group G, we call P a *Schur σ-ancestor group*. Note that a Schur σ-ancestor group is necessarily a finite p-group with a GI-automorphism (though these conditions are not sufficient). The Schur σ-ancestor groups are exactly those presented as $Q_c(F_g)/\langle\langle r_1,\ldots,r_g\rangle\rangle$ for some $r_1,\ldots,r_g \in X_c$. This is because one can choose an irredundant lift of the relations from X_c to X to give a Schur σ-group [BBH16]. In particular, for any Schur σ-ancestor group G of p-class c, we have that $\mu_{\mathrm{BBH},c}(G) > 0$.

3.1 Choice of GI-automorphisms

It might seem strange at first that we do not include the choice of GI-automorphism with our data of a Schur σ-group or Schur σ-ancestor group. However, we have the following proposition.

Proposition 3.1 [Hal34, § 1.3]. *Any two GI-automorphisms of a finitely generated pro-p group G are conjugate in* $\mathrm{Aut}(G)$.

If G and H are finitely generated pro-p groups, we define $\mathrm{Sur}_\sigma(G,H)$ to be the continuous surjections from G to H that take some particular choice of GI-automorphism for G to some particular choice of GI-automorphism for H. We define $\mathrm{Aut}_\sigma(G)$ similarly. These definitions of course depend on the particular choice of GI-automorphisms, but in this paper we will be concerned mostly with the size of these sets, and by Proposition 3.1 their sizes do not depend on these choices.

3.2 Choice of generators

The description of μ_{BBH} above actually gives a finer measure on the set of isomorphism classes of Schur σ-groups *with* a choice of GI-automorphism and minimal generating set inverted by that automorphism. We will later take advantage of this generating set, though for simplicity we do not introduce notation for this finer measure.

4. Boston–Bush–Hajir moments

We now determine the moments of the measure μ_{BBH} as stated in Theorem 1.3.

Theorem 4.1 (Moments of μ_{BBH}). *Let H be a finite p-group of p-class c with a GI-automorphism σ. Then*

$$\int_G |\mathrm{Sur}_\sigma(G,H)|\, d\mu_{\mathrm{BBH}} = \sum_{G \text{ Schur } \sigma\text{-ancestor of } p\text{-class } c} \mu_{\mathrm{BBH},c}(G)|\mathrm{Sur}_\sigma(G,H)| = 1.$$

Note the hypothesis that σ is *GI* on H does not place any real restriction, because if we have a surjection $G \to H$ that takes a GI-automorphism σ_G on G to any automorphism σ_H on H, then σ_H must also be GI.

Let H be a finite p group with an order-2 automorphism σ. We write

$$Z(H) = \{g \in H \mid \sigma(g) = g\}$$

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

and $Y(H) = \{g \in H \mid \sigma(g) = g^{-1}\}$. This notation implicitly depends on σ. We now prove several lemmas that will be used in the proof of Theorem 4.1.

Lemma 4.2. *Let G be a finite p-group with an order-2 automorphism σ. Then $|G| = |Y(G)|\,|Z(G)|$.*

Proof. This is [Gor07, Theorem 3.5 (p. 180) of ch. 5]. □

Lemma 4.3. *Let G and H be finite p-groups, each with an order-2 automorphism σ, and let $\phi : G \to H$ be a σ-equivariant surjection. Then $\phi : Z(G) \to Z(H)$ is a surjection.*

Proof. Associated to the exact sequence $1 \to \ker(\phi) \to G \to H \to 1$ is the exact sequence

$$\cdots \to H^0(\langle\sigma\rangle, G) \to H^0(\langle\sigma\rangle, H) \to H^1(\langle\sigma\rangle, \ker(\phi)) \to \cdots .$$

The first and second terms are $Z(G)$ and $Z(H)$ respectively. The last term is $H^1(\langle\sigma\rangle, \ker(\phi))$, which vanishes by the Schur–Zassenhaus theorem since p is odd. □

Lemma 4.4. *Let G and H be finite p-groups, each with an order-2 automorphism σ, and let $\phi : G \to H$ be a σ-equivariant surjection with kernel K. Then $Z(K) = K \cap Z(G)$ and $Y(K) = K \cap Y(G)$, and $|Y(K)| = |Y(G)|/|Y(H)|$.*

Proof. The first two claims are clear. Using the above two lemmas, we then observe

$$|Y(K)| = \frac{|K|}{|Z(K)|} = \frac{|G|/|H|}{|Z(G)|/|Z(H)|} = \frac{|Y(G)|}{|Y(H)|},$$

which proves the final claim. □

Lemma 4.5. *Let H be a finite p-group with GI-automorphism σ. Then the elements of $Y(H)$ are equidistributed in $H/\Phi(H)$. That is, any two cosets in H of $\Phi(H)$, when intersected with $Y(H)$ have the same number of elements.*

Proof. We consider the maps of sets $f : H \to Y(H)$ given by $f(g) = g^{-1}\sigma(g)$ and $\pi : Y(H) \to H/\Phi(H)$ the composition of the inclusion and quotient maps $Y(H) \to H \to H/\Phi(H)$.

Then the composition $\pi f : H \to H/\Phi(H)$ sends $g \mapsto g^{-2}$ since σ acts by inversion on $H/\Phi(H)$. This is a homomorphism since $H/\Phi(H)$ is abelian, and a surjection since $H/\Phi(H)$ has odd order. Thus the fibers of πf are of equal size. Further, the fibers of f are cosets of $Z(H)$ and thus are also of equal size. Also, since for any $g \in H$, $g\Phi(H) \cap Y(H) = \pi^{-1}(g)$, it suffices to show the fibres of π have equal sizes, which now follows. □

Lemma 4.6. *Let H be a finite p-group of generator rank r with a GI-automorphism σ. Then*

$$|\mathrm{Sur}_\sigma(F_d, H)| = \frac{|Y(H)|^d (p^d - p^{r-1}) \cdots (p^d - 1)}{p^{dr}}.$$

Proof. A homomorphism $F_d \to H$ is σ-equivariant if and only if it sends each of the d generators of F_d to an element of $Y(H)$, and so there are $|Y(H)|^d$ such maps. By the Burnside basis theorem, such a homomorphism is surjective if and only if its composition with the quotient map is surjective to $H/\Phi(H)$. Since the elements of $Y(H)$ are equidistributed in $H/\Phi(H)$,

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

the proportion of σ-equivariant homomorphisms $F_d \to H$ that are surjective is the same as the proportion of d-tuples from $H/\Phi(H) \simeq (\mathbb{Z}/p\mathbb{Z})^r$ that span this $\mathbb{Z}/p\mathbb{Z}$-vector space, which is easily computed to be $(p^d - p^{r-1}) \cdots (p^d - 1)/p^{dr}$. □

Proof of Theorem 4.1. Since a surjection from G to H factors through $Q_c(G)$, we see that $f(G) = |\mathrm{Sur}_\sigma(G, H)|$ is in fact a measurable function and that the first equality is by definition of the two measures.

Let H have generator rank r. The random group G is constructed first by picking a random generator rank d for G according to the Cohen–Lenstra measure, and then taking a random quotient of F_d. Certainly, any surjection $G \to H$ lifts uniquely to a surjection $F_d \to H$. From Lemma 4.6 we see there are $|Y(H)|^d (p^d - p^{r-1}) \cdots (p^d - 1)/p^{dr}$ σ-equivariant surjections $F_d \to H$. A surjection $\phi : F_d \to H$ factors through G if and only if the d random relations in $Y(\Phi(F_d))$ that present G are in $\ker(\phi)$, the probability of which we now compute. Since H is p-class c, we may equivalently take the random relations in $Y(\Phi(F_d)/P_c(F_d))$.

Let $F := F_d/P_c(F_d)$. The probability that a random relation in $X_c = Y(\Phi(F))$ is in $\ker(\phi)$ is $|\ker(\phi) \cap Y(\Phi(F))|/|Y(\Phi(F))|$. Applying Lemma 4.4 to the surjection $\phi : \Phi(F) \to \Phi(G)$, we see that $|\ker(\phi) \cap Y(\Phi(F))|/|Y(\Phi(F))| = |Y(\Phi(G))|^{-1}$. Also, applying Lemma 4.4 to the quotient $G \to G/\Phi(G)$, we have that $|Y(\Phi(G))| = |Y(G)|/p^r$, since σ acts on all of $G/\Phi(G)$ by inversion. Thus, the probability that d random relations are in $\ker(\phi)$, and so the map ϕ factors through the random G, is $p^{dr}/|Y(H)|^d$.

Multiplying by the number of σ-equivariant surjections $F_d \to H$, we find that among generator rank d groups G, the expected number of σ-equivariant surjections to H is $(p^d - p^{r-1}) \cdots (p^d - 1)$, which is the number of surjections from a rank d abelian p-group to $(\mathbb{Z}/p\mathbb{Z})^r$. Thus the expected number of σ-equivariant surjections is

$$\sum_{d \geqslant 0} \mu_{\mathrm{CL}}(d)(p^d - p^{r-1}) \cdots (p^d - 1) = \sum_A \mu_{\mathrm{CL}}(A)|\mathrm{Sur}(A, (\mathbb{Z}/p\mathbb{Z})^r)| = 1,$$

by the moments formula for the Cohen–Lenstra measure. □

In fact, we will see in Theorem 4.9 that the moments where H is a Schur σ-ancestor group characterize μ_{BBH} as a measure on Ω. At each p-class, showing the moments characterize the measure amounts to inverting an infinite-dimensional matrix. Our method to invert this matrix can be seen as a generalization of the method of [EVW16, Lemma 8.2], which proves that the moments characterize the Cohen–Lenstra measure on finite abelian p-groups. First we need an infinite-dimensional linear algebra lemma, since our infinite matrices are not quite as simple as those in [EVW16, Lemma 8.2].

Lemma 4.7. *Let $a_{i,j}$ be non-negative real numbers indexed by pairs of natural numbers i, j, such that for all i we have $a_{i,i} = 1$, and also $\sup_i \sum_j a_{ij} < 2$. Let x_j, y_j be non-negative reals indexed by natural numbers j. If for all i,*

$$\sum_j a_{i,j} x_j = \sum_j a_{i,j} y_j = 1,$$

then $x_j = y_j$ for all j.

Proof. Note that $x_i = a_{ii} x_i \leqslant \sum_j a_{i,j} x_j \leqslant 1$. Similarly $0 \leqslant y_i \leqslant 1$. Let $d_i = x_i - y_i$. Let $a = \sup_i \sum_j a_{ij} < 2$. Let $s = \sup_i |d_i|$, so $0 \leqslant s \leqslant 1$. For each i, we have $\sum a_{ij} d_j = 0$, so $d_i = -\sum_{j \neq i} a_{ij} d_j$. So, $|d_i| \leqslant \sum_{j \neq i} a_{ij} |d_j|$. Taking the supremum over i yields $s \leqslant (a-1)s$. Since $a - 1 < 1$, so $s = 0$. Thus $x_i = y_i$ for all i. □

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

Next, we will prove a formula for $\mu_{\mathrm{BBH}}(\{G \mid Q_c(G) \simeq P\})$ for a given Schur σ-ancestor group P. The formula combines [BBH16, Theorems 2.25 and 2.29], which are subject to a further conjecture called KIP, but we prove below that the combined formula is not conjectural. For the formula, we will need one further invariant of p-groups. For a finite p-group G of p-class c presented as F/R, where F is a free group of $d(G)$ generators, then $h(G)$ is defined to be the dimension of the quotient of R by the topological closure of the subgroup $R^p[F,R]P_c(F)$ (by [O'B90] and [BBH16, Remark 2.4] the quantity does not depend on the choice of presentation).

Alternatively, the p-groups of p-class $\leqslant c$ form a variety of groups whose free objects are precisely the groups $Q_c(F_d)$. For a group G in this variety, we can let $h_c(G)$ be the number of relators required to present G in this variety. If G is p-class c, then $h_c(G) = h(G)$ and if G is p-class smaller than c, then $h_c(G) = r(G)$.

Lemma 4.8. *Fix a c. Let $g = d(G)$ and $h = h_c(G)$. We have*

$$\frac{\mu_{\mathrm{BBH}}(\{G \mid Q_c(G) \simeq P\})}{\mu_{\mathrm{CL}}(g)} = \frac{p^{g^2}}{|\mathrm{Aut}_\sigma(G)|} \prod_{k=1}^{g}(1-p^{-k}) \prod_{k=1+g-h}^{g}(1-p^{-k}).$$

Proof. Let $F_c = Q_c(F_g)$. We need to compute the sum of the probabilities that a given g-tuple of relations $v \in X_c^g$ generates $\overline{R}$ as a normal subgroup of F_c, where $\overline{R}$ runs over all normal subgroups of F_c with quotient G. The key thing to note here is that since each element of X_c is inverted by σ, any subgroup generated by elements of X_c is σ-invariant, as is the normal closure of such a subgroup. Thus if $\overline{R}$ is a normal subgroup of F_c that is not σ-invariant, then the probability that is generated as a normal subgroup by relations from X_c is 0. In [BBH16], the conjectural property KIP (kernel invariance property) was assumed to ensure that every normal subgroup with quotient G is σ-invariant. We do not assume this, since by the above remark we can restrict our attention to the set of σ-invariant normal subgroups with quotient G.

The number of σ-invariant normal subgroups of F_c with quotient G is $|\mathrm{Sur}_\sigma(F_c, G)|/|\mathrm{Aut}_\sigma(G)|$, by counting the quotient maps and dividing by how often maps give isomorphic quotients. (There are similarly $|\mathrm{Sur}(F_c, G)|/|\mathrm{Aut}(G)|$ normal subgroups with quotient G, but if there are any that are not σ-invariant we have already seen they have 0 probability of being generated by our relations in X_g.) The probability that a g-tuple of relations $v \in X_c^g$ generates a σ-invariant $\overline{R}$ as a normal subgroup can be computed by the earlier methods of [BBH16]. We give a slightly alternative treatment here.

First note that by Lemma 4.6, $|\mathrm{Sur}_\sigma(F_c, G)| = |Y(G)|^g \prod_{k=1}^{g}(1-p^{-k})$, since every such surjection from the free pro-p group F_g on g generators factors through F_c. As for the probability that $v \in X_c^g$ normally generates $\overline{R}$, this happens if and only if its image generates the $\mathbb{F}_p$-vector space $V = \overline{R}/\overline{R}^*$, where R is the preimage of $\overline{R}$ in F_g, R^* is the topological closure of $R^p[F_g, R]$, and $\overline{R}^* = P_c(F_g)R^*/P_c(F_g)$ [Gru76, Proposition 2.8]. When G is p-class c, the dimension of V is h (by definition of h). When G is p-class $< c$, we have $P_{c-1}(F_g) \subset R$ and so $P_c(F_g)$ is a subgroup of R^*. Then $V = R/R^*$, which has dimension $r(G)$. Let $s = \dim V$, which we have just determined in each case. The number of g-tuples generating V is $\prod_{k=1}^{s}(p^g - p^{s-k})$ and so we just need the size of the intersection of X_c with a fiber of the quotient map $r : \overline{R} \to V$.

We claim each of these has $|\overline{R}^*|/|Z(\overline{R})|$ elements. This follows by considering the map f of Lemma 4.5, defined by $f(g) = g^{-1}\sigma(g)$. Since V is abelian, $f \circ r = -2r$, whose fibers have the same size as those of r, namely $|\overline{R}^*|$, since p is odd. On the other hand, $f \circ r = r \circ f$, the size of the fibers of which are the size of those of r times those of f. This latter term is $|Z(\overline{R})|$ by Lemma 4.2. Putting these facts together establishes the claim.

To recap, the desired measure is the sum over $|Y(G)|^g \prod_{k=1}^{g}(1-p^{-k})/|\mathrm{Aut}_\sigma(G)|$ terms of the number of v in X_c^g normally generating each $\overline{R}$, which we just found to be $\prod_{k=1}^{s}(p^g - p^{s-k})(|\overline{R}^*|/|Z(\overline{R})|)^g$, divided by the total number of v, namely $|X_c|^g$. In other words,

$$\prod_{k=1}^{s}(p^g - p^{s-k})\prod_{k=1}^{g}(1-p^{-k})\frac{(|\overline{R}^*|/|Z(\overline{R})|)^g|Y(G)|^g}{|\mathrm{Aut}_\sigma(G)|\,|X_c|^g}.$$

It remains to show that $|Y(G)|\,|\overline{R}^*|/(|Z(\overline{R})|\,|X_c|) = p^{g-s}$. This follows from Lemma 4.4, which says that $|Y(F_c)| = |Y(G)|\,|Y(\overline{R})|$ and $|Y(F_c)| = |Y(\Phi(F_c))|\,|Y(F_c/\Phi(F_c))| = |X_c|p^g$. Thus, $|X_c| = |Y(G)|\,|Y(\overline{R})|p^{-g}$. Combining this with $|Y(\overline{R})|\,|Z(\overline{R})| = |\overline{R}|$ (Lemma 4.2) and $|\overline{R}|/|\overline{R}^*| = p^s$ gives the result. □

Theorem 4.9 (Moments characterize μ_{BBH}). *Let ν be a measure on Ω such that for every Schur σ-ancestor group H,*

$$\int_G |\mathrm{Sur}_\sigma(G,H)|\,d\nu = 1.$$

Then $\nu = \mu_{\mathrm{BBH}}$.

Note that Schur σ-ancestor groups are a proper subset of finite p-groups with GI-automorphisms, so this theorem does not require all of the moments determined in Theorem 4.1.

Proof. By Carathéodory's theorem, a measure ν on Ω is determined by the measures $\nu(\{G \mid Q_c(G) \simeq S\})$ for all Schur σ-ancestor groups S. If G is a Schur σ-group, then $Q_c(G)$ is either a Schur σ-ancestor group of p-class c or a Schur σ-group of p-class $< c$. (This is because if $Q_c(G)$ is p-class $< c$ then $Q_c(G) = G$.) Let $\mathcal{S}$ be the set of isomorphism classes of groups that are either a Schur σ-ancestor group of p-class c or a Schur σ-group of p-class $<c$.

For H a Schur σ-ancestor group of p-class c, we have that

$$\sum_{S\in\mathcal{S}} \nu(\{G \mid Q_c(G) \simeq S\})|\mathrm{Sur}_\sigma(S,H)| = 1$$

and

$$\sum_{S\in\mathcal{S}} \mu_{\mathrm{BBH}}(\{G \mid Q_c(G) \simeq S\})|\mathrm{Sur}_\sigma(S,H)| = 1.$$

We can index $\mathcal{S}$ by natural numbers $S_1, S_2, \ldots$. We then apply Lemma 4.7 with

$$a_{i,j} = \frac{|\mathrm{Sur}_\sigma(S_j,S_i)|}{|\mathrm{Aut}_\sigma(S_j)|}$$

and $x_j = \nu(\{G \mid Q_c(G) \simeq S_j\})|\mathrm{Aut}_\sigma(S_j)|$ and $y_j = \mu_{\mathrm{BBH}}(\{G \mid Q_c(G) \simeq S_j\})|\mathrm{Aut}_\sigma(S_j)|$, which will prove the proposition. We must verify that $\sum_j a_{i,j} < 2$.

Using the explicit formulae for $\mu_{\mathrm{CL}}(d)$ (from [CL84]) and for μ_{BBH} (from Lemma 4.8), we have that

$$\mu_{\mathrm{BBH}}(\{G \mid Q_c(G) \simeq S_j\}) = \frac{\mu_{\mathrm{CL}}(d(S_j))p^{d(S_j)^2}}{|\mathrm{Aut}_\sigma(S_j)|}\prod_{k=1}^{d(S_j)}(1-p^{-k})\prod_{k=1+d(S_j)-h_c(S_j)}^{d(S_j)}(1-p^{-k})$$

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

$$= \frac{\prod_{k\geqslant 1}(1-p^{-k})\prod_{k=1}^{d(S_j)}(1-p^{-k})^{-2}}{|\mathrm{Aut}_\sigma(S_j)|}\prod_{k=1}^{d(S_j)}(1-p^{-k})\prod_{k=1+d(S_j)-h_c(S_j)}^{d(S_j)}(1-p^{-k})$$

$$= \frac{1}{|\mathrm{Aut}_\sigma(S_j)|}\prod_{k\geqslant 1}(1-p^{-k})\prod_{k=1}^{d(S_j)}(1-p^{-k})^{-1}\prod_{k=1+d(S_j)-h_c(S_j)}^{d(S_j)}(1-p^{-k}).$$

When S_j is p-class c, we have that $h_c(S_j)=h(S_j)$, and since S_j is a Schur σ-ancestor, it is $Q_c(G)$ for some Schur σ-group G. Since $r(G)=d(G)=d(S_j)$, and $r(G)\geqslant h(S_j)$ [BN06, Proposition 2], we have $d(S_j)\geqslant h_c(S_j)$. When S_j is a Schur σ-group, we have that $h_c(S_j)=r(S_j)=d(S_j)$. In either case, we conclude that

$$\mu_{\mathrm{BBH}}(\{G \mid Q_c(G)\simeq S_j\}) \geqslant \frac{1}{|\mathrm{Aut}_\sigma(S_j)|}\prod_{k\geqslant 1}(1-p^{-k}).$$

For all $p\geqslant 3$, we have that $\prod_{k\geqslant 1}(1-p^{-k})>0.53$ and so

$$\frac{1}{|\mathrm{Aut}_\sigma(S_j)|} < 1.9\mu_{\mathrm{BBH}}(\{G \mid Q_c(G)\simeq S_j\}).$$

Thus,

$$\sup_i \sum_j a_{i,j} = \sup_i \sum_j \frac{|\mathrm{Sur}_\sigma(S_j,S_i)|}{|\mathrm{Aut}_\sigma(S_j)|}$$
$$\leqslant 1.9 \sup_i \sum_j \mu_{\mathrm{BBH}}(\{G \mid Q_c(G)\simeq S_j\})|\mathrm{Sur}_\sigma(S_j,S_i)| \leqslant 1.9. \qquad \square$$

5. Moments as an extension counting problem

Let Q be a global field with a choice of place ∞. (We are mainly interested in $Q=\mathbb{Q}$ or $\mathbb{F}_q(t)$ with the usual infinite place.) We fix a separable closure $\bar{Q}_\infty$ of the completion Q_∞. Then, inside $\bar{Q}_\infty$ we have the separable closure $\bar{Q}$ of Q. This gives a map $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty)\to\mathrm{Gal}(\bar{Q}/Q)$, and in particular distinguished decomposition and inertia groups in $\mathrm{Gal}(\bar{Q}/Q)$ at ∞ (as opposed to just a conjugacy classes of subgroups).

As in § 2, when $K\subset\bar{Q}$ with K/Q a separable, quadratic extension, we let $K^{\mathrm{un},\infty}\subset\bar{Q}$ be the maximal extension of K that is unramified everywhere and split completely at ∞. We let $G_K^{\mathrm{un},\infty}:=\mathrm{Gal}(K^{\mathrm{un},\infty}/K)$. We note that in $\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$ the inertia group at ∞ has order dividing 2 by Lemma 2.2. Thus if K is ramified at ∞, we have a distinguished non-trivial inertia element $i_{K,\infty}\in\mathrm{Gal}(K^{\mathrm{un},\infty}/Q)$. As noted earlier, an automorphism that has order dividing 2 is called an *involution*. Conjugation by $i_{K,\infty}$ gives an involution of $G_K^{\mathrm{un},\infty}$, and we let this conjugation be our chosen automorphism σ of $G_K^{\mathrm{un},\infty}$. (Note this is a more specific choice than we made in § 2 under different hypotheses.)

Recall, for any finite group H with an involution σ, we write $\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty},H)$ for the continuous surjections taking conjugation by $i_{K,\infty}$ to σ. We let $G=H\rtimes_\sigma C_2$, and we denote the generator of C_2 by σ (a convenient overloading of notation). Let c be the set of elements of $G\backslash H$ of order 2.

We define (as in [EVW12, § 10.2]) a *marked* (G,c) *extension* of Q to be (L,π,m) such that L/Q is a Galois extension of fields, π is an isomorphism $\pi:\mathrm{Gal}(L/Q)\simeq G$ such that all inertia groups in $\mathrm{Gal}(L/Q)$ (except for possibly the one at ∞) have image in $\{1\}\cup c$, and m,

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

the *marking*, is a homomorphism $L_\infty := L \otimes_Q Q_\infty \to \bar{Q}_\infty$. Note that restriction to L gives a bijection between homomorphisms $L_\infty \to \bar{Q}_\infty$ and homomorphisms $L \to \bar{Q}$. Also, note that the condition that an inertia group in $\mathrm{Gal}(L/Q)$ has image in $\{1\} \cup c$ is equivalent to requiring that it has trivial intersection with $\pi^{-1}(H)$ because any element in $G\backslash(\{1\} \cup c)$ is either in H or has square non-trivial in H. Two marked (G, c) extensions (L_1, π_1, m_1) and (L_2, π_2, m_2) are isomorphic when there is an isomorphism $L_1 \to L_2$ taking π_1 to π_2 and m_1 to m_2. The marking m in a marked (G, c) extension (L, π, m) gives a map $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to \mathrm{Gal}(L/Q)$. Composing with π we get an *infinity type* $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to G$. Such a homomorphism is called ramified if the image of inertia is non-trivial.

Note that in each isomorphism class of marked (G, c) extensions of Q, there is a distinguished element such that $L \subset \bar{Q}$ and $m|_L$ is the inclusion map.

Theorem 5.1. *Let Q be a global field with a choice of place ∞. Let H be a finite group with involution σ, let $G := H \rtimes_\sigma C_2$, and let c be the set of order-2 elements of $G\backslash H$. Let $\phi : \mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to G$ be a ramified homomorphism with image $\langle(1, \sigma)\rangle$. There is a bijection between*

$$\big\{(K, f) | K \subset \bar{Q}, [K : Q] = 2, K_\infty/Q_\infty \textit{ the quadratic extension given by } \ker(\phi), f \in \mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)\big\}$$

and

$$\{\textit{isomorphism classes of marked } (G, c) \textit{ extensions } (L, \pi, m) \textit{ of } Q \textit{ with infinity type } \phi\}.$$

In this bijection, we have $\mathrm{Disc}(L) = \mathrm{Disc}(K)^{|H|}$.

Proof. Given a (K, f), we have that $\ker(f)$ gives a subfield of $L \subset K^{\mathrm{un},v} \subset \bar{Q}$ and we have $f : \mathrm{Gal}(L/K) \simeq H$. We see that $\mathrm{Gal}(L/K)$ is an index 2 subgroup of $\mathrm{Gal}(L/Q)$, and $i_{K,\infty}$ is an order-2 element of $\mathrm{Gal}(L/Q)\backslash \mathrm{Gal}(L/K)$. From the condition on the surjection f, we have that f takes the conjugation action of $i_{K,\infty}$ on $\mathrm{Gal}(L/K)$ to the involution σ on H. Thus we can lift f to $\pi : \mathrm{Gal}(L/Q) \simeq G$ with $i_{K,\infty} \mapsto (1, \sigma)$. We let the marking m be the map $L_\infty \to \bar{Q}_\infty$ induced by the identity on $L \subset \bar{Q} \subset \bar{Q}_\infty$. Since $L \subset K^{\mathrm{un},\infty}$, all inertia subgroups of $\mathrm{Gal}(L/Q)$ have image under π in $\{1\} \cup c$. The infinity type $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to G$ factors through the map π. Since the index 2 subgroup $\mathrm{Gal}(\bar{Q}_\infty/K_\infty)$ has trivial image (it factors through $\mathrm{Gal}(L/K)$, and L/K is split completely at ∞), the infinity type of m factors through the order-2 group $\mathrm{Gal}(K_\infty/Q_\infty)$. Since, by construction of π, the inertia group $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty)$ has image $\langle(1, \sigma)\rangle$, it follows that the infinity type is $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to \mathrm{Gal}(K_\infty/Q_\infty) \simeq \langle(1, \sigma)\rangle$, which is ϕ.

Given an isomorphism class of marked (G, c) extensions (L, π, m) of Q with infinity type ϕ, we take the representative for which $L \subset \bar{Q}$ and $m|_L$ is the identity map. Then we let $K \subset \bar{Q}$ be the fixed field of $\pi^{-1}(H)$. From the infinity type, we see that L/K is split completely at ∞, and that K/Q is ramified at ∞ such that K_∞ corresponds to $\ker(\phi)$. By the fact that (L, π, m) is a (G, c) extension of infinity type ϕ, it follows that $L \subset K^{\mathrm{un},\infty}$, so we get a surjection $f : G_K^{\mathrm{un},\infty} \to \mathrm{Gal}(L/K) \xrightarrow{\pi} H$. From the infinity type, we see that π takes $i_{K,\infty} \mapsto (1, \sigma)$, so we get that $f \in \mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)$.

If we start with (K, f), then by construction the fixed field of the $\pi^{-1}(H)$ from our constructed (L, π) is K, and the restriction of π to $\mathrm{Gal}(L/K)$ is f. So if we apply both these constructions we return to the same (K, f). On the other hand, if we start with (L, π, m) (such that m is the identity), L is the fixed field of the constructed morphism f, and π is determined by the constructed f and the image of $i_{K,\infty}$, and so if we apply both these constructions we return to (L, π, m). ☐

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

6. Applying methods of Ellenberg–Venkatesh–Westerland to the extension counting problem

Theorem 1.5 will follow from Corollary 6.5 in this section. We will prove this result using a method and many results due to Ellenberg, Venkatesh and Westerland in papers [EVW16, EVW12]. The method counts extensions of function fields by considering this as a problem of counting $\mathbb{F}_q$ points on a moduli space of curves with maps to $\mathbb{P}^1$, applying the Grothendieck–Lefschetz trace formula to count these points, and using results from topology to bound the dimensions of the cohomology groups.

6.1 Group theory computation

In this section, we will prove a lemma in group theory that will be central to proving Theorem 1.5. This lemma will count $\mathbb{F}_q$-rational components in a moduli space on which we will eventually count points.

First we will define the *universal marked central extension* $\tilde{G}$ of a finite group G for a union c of conjugacy classes of G, following [EVW12, § 7]. Let C be a Schur cover of G so we have an exact sequence

$$1 \to H_2(G, \mathbb{Z}) \to C \to G \to 1$$

by the Schur covering map. For $x, y \in G$ that commute, let $\hat{x}$ and $\hat{y}$ be arbitrary lifts to C, and let $\langle x, y\rangle$ be the commutator $[\hat{x}, \hat{y}] \in C$, which actually lies in $H_2(G, \mathbb{Z})$ since x and y commute. It we take the quotient of the above exact sequence by all $\langle x, y\rangle$ for $x \in c$ and y commuting with x, we obtain an exact sequence

$$1 \to H_2(G, c) \to \tilde{G}_c \to G \to 1,$$

which is still a central extension. Let G^{ab} denote the abelianization of H. The universal marked central extension is $\tilde{G} = \tilde{G}_c \times_{G^{\mathrm{ab}}} \mathbb{Z}^{c/G}$, where c/G denotes the set of conjugacy classes in c and the map $\mathbb{Z}^{c/G} \to G^{\mathrm{ab}}$ sends each standard generator to an element of the associated conjugacy class. We have a map $\tilde{G} \to G$, given through projecting to the first factor. (See [EVW12, § 7] for why this is called a universal marked central extension.)

Lemma 6.1. *Let H be an odd finite group with a GI-automorphism σ, and $G = H \rtimes_\sigma C_2$. Let c be the (single) conjugacy class of order-2 elements. Let q be a power of a prime and n be an odd integer. If $(q, 2|H|) = 1$ and $(q-1, |H|) = 1$, then for each $y \in c$, there is exactly 1 element $x \in \tilde{G}_c$ such that $(x, n) \in \tilde{G}$, and x has image y in G, and $x^q = x$.*

Proof. We have that $|\tilde{G}_c| = 2|H||H_2(G, c)|$ and that $H_2(G, \mathbb{Z})$ is a quotient of $H_2(H, \mathbb{Z})$ by [EVW12, Example 9.3.2]. Thus since $|H|$ is relatively prime to $2(q-1)$, we have that $|H_2(G, \mathbb{Z})|$ is as well and thus $|H_2(G, c)|$ is as well. Since $|\tilde{G}_c|/2$ is relatively prime to $q-1$, we have that for $x \in \tilde{G}_c$, $x^q = x$ if and only if $x^2 = 1$.

Let $w \in \tilde{G}_c$ be in the inverse image of y. Then we ask for which $k \in H_2(G, c)$ is wk of order 2. Since $H_2(G, c) \to \tilde{G}_c$ is central, we have $(wk)^2 = w^2k^2$, and note $w^2 \in H_2(G, c)$ since $y^2 = 1$. Since $H_2(G, c)$ is an odd abelian group, there is exactly one $k \in H_2(G, c)$ such that $w^2k^2 = 1$. Let $x = wk$ for this k, which is the only possible x satisfying the conditions of the lemma. Also, note that $(x, n) \in \tilde{G}$ since x and n have image of the class of y in G^{ab}, proving the lemma. ☐

6.2 Properties of the Hurwitz scheme constructed by Ellenberg, Venkatesh and Westerland

In this theorem, we recall the Hurwitz scheme constructed by Ellenberg, Venkatesh and Westerland to study extensions of $\mathbb{F}_q(t)$ and its properties.

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

Theorem 6.2 (Ellenberg, Venkatesh and Westerland). *Let H be an odd finite group with GI-automorphism σ, and let $G := H \rtimes_\sigma C_2$. Let c be the elements of G of order 2. Let $\mathbb{F}_q$ be a finite field with q relatively prime to $|G|$. When G is center-free, there is a Hurwitz scheme $\mathsf{CHur}_{G,n}$ over $\mathbb{Z}[|G|^{-1}]$ constructed in [EVW12, § 8.6.2][1] with the following properties.*

(i) *We have $\mathsf{CHur}_{G,n}$ is a finite étale cover of the relatively smooth n-dimensional configuration space Conf^n of n distinct unlabeled points in $\mathbb{A}^1$ over $\operatorname{Spec} \mathbb{Z}[|G|^{-1}]$.*

(ii) *The scheme $\mathsf{CHur}_{G,n}$ has an open and closed subscheme $\mathsf{CHur}^{c,c}_{G,n}$ such that there is a bijection between:*

(a) *isomorphism classes of marked (G, c)-extensions L of $\mathbb{F}_q(t)$ of $\operatorname{Nm}\operatorname{Disc}(L) = q^{(n+1)|H|}$ and an infinity type ϕ such that $\phi(F_\Delta) = 1$ and $\operatorname{im}\phi$ is of order 2 and in $c \cup \{1\}$ (where F_Δ is a lift of the Frobenius automorphism to $\mathrm{Gal}(\bar{Q}_\infty/Q_\infty)$ that acts trivially on $\mathbb{F}_q((t^{-1/\infty})))$;*

(b) *points of $\mathsf{CHur}^{c,c}_{G,n}(\mathbb{F}_q)$ [EVW12, § 10.4].*

(iii) *We have $\mathsf{CHur}_{G,n}(\mathbb{C})$ is homotopy equivalent to a topological space $\mathrm{CHur}_{G,n}$ [EVW12, § 8.6.2], such that for any field k of characteristic relatively prime to $|G|$, there is a constant C such that for all $i \geqslant 1$ and for all n we have $\dim H^i(\mathrm{CHur}_{G,n}, k) \leqslant C^i$ [EVW16, Proposition 2.5 and Theorem 6.1].*

(iv) *Given G, for n sufficiently large and all q with $(q, G) = 1$, the* Frob *fixed components of $\mathsf{CHur}^{c,c}_{G,n} \otimes_{\mathbb{Z}[|G|^{-1}]} \bar{\mathbb{F}}_q$ are in bijection with elements $(x, n) \in \tilde{G}$ such that $x^q = x$ and x has image of order 2 in G [EVW12, Theorem 8.7.3]. (The requirement that x has image of order 2 in G ensures the monodromy at ∞ is in c.)*

Remark 6.3. The scheme $\mathsf{CHur}^{c,c}_{G,n} \subset \mathsf{CHur}_{G,n}$ comes from restricting to the parametrization of covers of $\mathbb{P}^1$ all of whose local inertia groups have image in $c \cup \{1\}$. We use two c superscripts because [EVW12] uses a single c superscript to denote when this restriction is made only over points in $\mathbb{A}^1 \subset \mathbb{P}^1$. The argument that $\mathsf{CHur}^{c,c}_{G,n} \subset \mathsf{CHur}_{G,n}$ is an open and closed subscheme is as in [EVW16, § 7.3]. Our description of the components requires a bit of translation from that in [EVW12, Theorem 8.7.3]. They biject the components with $\hat{\mathbb{Z}}^\times$ equivariant functions from topological generators of $\varprojlim \mu_n$ (taken over n relatively prime to q) to the preimage of c in $\tilde{G}$ that are fixed by the discrete action of Frob. By choosing any topological generator of $\varprojlim \mu_n$, its image under a function to $\tilde{G}$ gives us a corresponding element of $\tilde{G}$. Using the definition of the discrete action and [EVW12, (9.4.1) and 9.3.2], we can see that under this correspondence $(x, n) \mapsto (x^q, n)$ describes the inverse of Frob.

6.3 Counting $\mathbb{F}_q$ points

In this section, we will count the $\mathbb{F}_q$ points of $\mathsf{CHur}^{c,c}$ in Theorem 6.4, and then use our Theorem 5.1 to translate that into a result about surjections from Galois groups G_K in Corollary 6.5, which will finally prove Theorem 1.5.

Theorem 6.4. *Given G and c as in Theorem 6.2, we have a constant C and a constant n_G such that for $q > C^2$, with $(q, |G|) = 1$ and $(q - 1, |G|/2) = 1$, and odd $n \geqslant n_G$,*

$$|\#\mathsf{CHur}^{c,c}_{G,n}(\mathbb{F}_q) - q^n \cdot \#c| \leqslant \frac{q^n}{\sqrt{q}/C - 1}.$$

[1] The paper [EVW12] has been temporarily withdrawn by the authors because of a gap which affects §§ 6, 12 and some theorems of the introduction of [EVW12]. That gap does not affect any of the results from [EVW12] that we use in this paper.

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press

Proof. Our theorem will follow by applying the Grothendieck–Lefschetz trace formula to $X := \mathsf{CHur}^{c,c}_{G,n} \otimes_{\mathbb{Z}[|G|^{-1}]} \mathbb{F}_q$. By Theorem 6.2(i), we have that X is smooth of dimension n. We have that $\dim H^i_{\mathrm{c,ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \dim H^{2n-i}_{\mathrm{ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ by Poincaré duality.

Next, we will relate $\dim H^j_{\mathrm{ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ to $\dim H^j(\mathsf{CHur}^{c,c}_{G,n}(\mathbb{C}), \mathbb{Q}_\ell)$ for some $\ell > n$. To compare étale cohomology between characteristic 0 and positive characteristic, we will use [EVW16, Proposition 7.7]. The result [EVW16, Proposition 7.7] gives an isomorphism between étale cohomology between characteristic 0 and positive characteristic in the case of a finite cover of a complement of a reduced normal crossing divisor in a smooth proper scheme. Though [EVW16, Proposition 7.7] is only stated for étale cohomology with coefficients in $\mathbb{Z}/\ell\mathbb{Z}$, the argument goes through identically for coefficients in $\mathbb{Z}/\ell^k\mathbb{Z}$, and then we can take the indirect limit and tensor with $\mathbb{Q}_\ell$ to obtain the result of [EVW16, Proposition 7.7] with $\mathbb{Z}/\ell\mathbb{Z}$ coefficients replaced by $\mathbb{Q}_\ell$ coefficients. So we apply this strengthened version to conclude that $\dim H^j_{\mathrm{ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \dim H^j_{\mathrm{ét}}((\mathsf{CHur}^{c,c}_{G,n})_{\mathbb{C}}, \mathbb{Q}_\ell)$. (As in [EVW16, proof of Proposition 7.8], we apply comparison to $\mathsf{CHur}^{c,c}_{G,n} \times_{\mathrm{Conf}^n} \mathrm{PConf}_n$, where PConf_n is the moduli space of n labeled points on $\mathbb{A}^1$ and is the complement of a relative normal crossings divisor in a smooth proper scheme [EVW16, Lemma 7.6]. Then we take S_n invariants to compare the étale cohomology of $\mathsf{CHur}^{c,c}_{G,n}$ across characteristics.) By the comparison of étale and analytic cohomology [SGA4(3), Exposé XI, Theorem 4.4] $\dim H^j(\mathsf{CHur}^{c,c}_{G,n}(\mathbb{C}), \mathbb{Q}_\ell) = \dim H^j_{\mathrm{ét}}((\mathsf{CHur}^{c,c}_{G,n})_{\mathbb{C}}, \mathbb{Q}_\ell)$.

By Theorem 6.2(iii), there is a constant C such that for all $j \geqslant 1$ and for all n, we have $\dim H^j(\mathsf{CHur}^{c,c}_{G,n}(\mathbb{C}), \mathbb{Q}_\ell) \leqslant C^j$. Thus $\dim H^j_{\mathrm{ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) \leqslant C^j$ for all $j \geqslant 1$. Thus using Poincaré duality, $\dim H^i_{\mathrm{ét},c}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) \leqslant C^{2n-i}$ for all $i < 2n$. By Theorem 6.2(iv) and Lemma 6.1, we have that X has $\#c$ components fixed by Frob for odd $n \geqslant n_G$ for some fixed n_G.

Then by the Grothendieck–Lefschetz trace formula we have

$$\#X(\mathbb{F}_q) = \sum_{j \geqslant 0} (-1)^j \operatorname{Tr}(\mathrm{Frob}|_{H^j_{\mathrm{c,ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)})$$

and also we know $\operatorname{Tr}(\mathrm{Frob}|_{H^{2n}_{\mathrm{c,ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)})$ is q^n times the number of components of X fixed by Frob. Since X is smooth, we have that the absolute value of any eigenvalue of Frob on $H^j_{\mathrm{c,ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ is at most $q^{j/2}$. Thus, for odd $n \geqslant n_G$,

$$\begin{aligned} |\#X(\mathbb{F}_q) - q^n \times \#c| &= \left| \sum_{0 \leqslant j < 2\dim X} (-1)^j \operatorname{Tr}(\mathrm{Frob}|_{H^j_{\mathrm{c,ét}}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)}) \right| \\ &\leqslant \sum_{0 \leqslant j < 2\dim X} q^{j/2} C^{2n-j} \\ &\leqslant q^n \sum_{1 \leqslant i} (\sqrt{q}/C)^{-i}. \end{aligned}$$

The theorem follows. □

We have $Q = \mathbb{F}_q(t)$ and $Q_\infty = \mathbb{F}_q((t^{-1}))$, for q odd. Unlike in the number field case, in which there is only one possible ramified quadratic extension of $\mathbb{Q}_\infty = \mathbb{R}$, here there are two ramified quadratic extensions of $Q_\infty = \mathbb{F}_q((t^{-1}))$. If $K/\mathbb{F}_q(t)$ is a quadratic extension, we say it is imaginary quadratic of type I if $K_\infty \simeq \mathbb{F}_q((t^{-1/2}))$ and of type II if $K_\infty \simeq \mathbb{F}_q(((\alpha t)^{-1/2}))$ for an $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_q^2$. Let IQ_n be the set of $K \subset \bar{Q}$ such that K is imaginary quadratic of type I and $\operatorname{Nm}\operatorname{Disc}(K) = q^{n+1}$. Let IQ'_n be the set of $K \subset \bar{Q}$ such that K is imaginary quadratic of type II and $\operatorname{Nm}\operatorname{Disc}(K) = q^{n+1}$.

Corollary 6.5. *Let H be an odd finite group with GI-automorphism σ such that $H \rtimes_\sigma C_2$ is center-free. As q ranges through powers of primes such that $(q, 2|H|) = 1$ and $(q-1, |H|) = 1$, we have*

$$\lim_{q\to\infty} \limsup_{\substack{n\to\infty \\ n \text{ odd}}} \frac{\sum_{K\in IQ_n} |\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|}{\# IQ_n} = 1.$$

The same result holds if we replace $\limsup$ *by* $\liminf$ *and/or replace* IQ_n *by* IQ_n'.

Theorem 1.5 then follows from Corollary 6.5 after noting that $H \rtimes_\sigma C_2$ is center-free if and only if the center of H contains no elements fixed by σ except the identity.

Proof. By Theorem 6.2(ii) the points $\mathsf{CHur}^{c,c}_{G,n}(\mathbb{F}_q)$ are in bijection with isomorphism classes of marked (G, c) extensions (L, π, m) of Q with certain infinity types ϕ. These infinity types are all G-conjugate, and there are $\#c$ of them. Let ϕ_0 be the infinity type such that $\phi(F_\Delta) = 1$ and $\operatorname{im}\phi = \langle(1, \sigma)\rangle$. Note that $\mathbb{F}_q((t^{-1/2}))$ is the imaginary quadratic extension given by $\ker(\phi_0)$.

Let $\phi : \mathrm{Gal}(\bar{Q}_\infty/Q_\infty) \to G$ be a ramified homomorphism with image $\langle(1, \sigma)\rangle$, let $g \in G$, and let ϕ^g denote the conjugation. Then isomorphism classes of marked (G, c) extensions (L, π, m) of Q with infinity type ϕ of a given discriminant are in bijection with isomorphism classes of marked (G, c) extensions (L, π, m) of Q with infinity type ϕ^g and that discriminant by sending (L, π, m) to (L, π^g, m). So, we have that

$$\#\mathsf{CHur}^{c,c}_{G,n}(\mathbb{F}_q) = \#c \cdot \#\big\{\text{isomorphism classes of marked } (G, c)\text{-extensions } L/\mathbb{F}_q(t) \text{ of infinity type } \phi_0 \text{ and } \operatorname{Nm}\operatorname{Disc}(L) = q^{(n+1)|H|}\big\}.$$

Further, by Theorem 5.1, we then conclude that

$$\#\mathsf{CHur}^{c,c}_{G,n}(\mathbb{F}_q) = \#c \cdot \big\{(K, f) \mid K \subset \bar{Q}, K \text{ imaginary quadratic type I}, f \in \mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H), \operatorname{Nm}\operatorname{Disc}(K) = q^{n+1}\big\}.$$

So by Theorem 6.4, we have a constant C, only depending on H, such that for $q \geqslant 4C^2$ and odd $n \geqslant n_G$

$$\left| \sum_{K\in IQ_n} |\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)| - q^n \right| \leqslant 2Cq^{n-1/2}.$$

Thus, for $q \geqslant 4C^2$ and all odd $n \geqslant n_G$

$$\frac{\sum_{K\in IQ_n} |\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|}{\# IQ_n} = \frac{q^n + O(q^{n-1/2})}{q^n - q^{n-1}} = 1 + O(q^{-1/2}).$$

It follows that the limit as $q \to \infty$, of the of $\limsup$ or $\liminf$, in odd n, of the lefthand side are both 1. For the case of IQ_n', we have a bijection $K \mapsto K \otimes_{\mathbb{F}_q(t)} \mathbb{F}_q(t)$ (where the map $\mathbb{F}_q(t) \to \mathbb{F}_q(t)$ is given by $t \mapsto \alpha t$, for some $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_q^2$) between IQ_n and IQ_n' that preserves $G_K^{\mathrm{un},\infty}$. □

6.4 Further results assuming a conjecture on the homology of Hurwitz spaces

The program developed by Ellenberg, Venkatesh and Westerland in [EVW12] aims to prove stronger results on the topology of Hurwitz spaces, from which corresponding stronger results on the point counts would follow. For example, HS_α [EVW12, § 11.1] is a conjecture on the homology of Hurwitz spaces for a given group G and conjugacy invariant subset c.

Theorem 6.6. *Let H be an odd finite group with GI-automorphism σ such that $H \rtimes_\sigma C_2$ is center-free. If HS_α holds for $G = H \rtimes_\sigma C_2$ and c the order-2 elements of G, then there is a q_0 such that for $q \geqslant q_0$, with $(q, 2|H|) = 1$ and $(q-1, |H|) = 1$, we have*

$$\limsup_{\substack{n\to\infty \\ n \text{ odd}}} \frac{\sum_{K\in IQ_n} |\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|}{\# IQ_n} = 1.$$

The same result holds if we replace IQ_n by IQ'_n.

Proof. We apply Theorem 5.1 and [EVW12, Theorem 11.1.1]. Lemma 6.1 shows that the quantity $B(L_\infty, \mathfrak{m})$ appearing in [EVW12, Theorem 11.1.1] is 1. Finally, we use that an étale G-extension L_∞ has $|G|/|\mathrm{Aut}_G(L_\infty)|$ corresponding infinity types and a G-extension has $|G|$ markings. □

7. Non-equivariant moments

While in this paper, we have asked about the equivariant moments, or averages of $|\mathrm{Sur}_\sigma(G_K^{\mathrm{un},\infty}, H)|$, one could naturally ask about non-equivariant moments, or averages of $|\mathrm{Sur}(G_K^{\mathrm{un},\infty}, H)|$. It turns out these non-equivariant moments reduce in a simple way to equivariant moments.

Let G be a group with a GI-automorphism σ. Then we have an injection

$$\begin{aligned} \mathrm{Sur}(G, H) &\to \mathrm{Hom}_\sigma(G, H\times H) \\ f &\mapsto f \times f\sigma, \end{aligned}$$

where the automorphism σ of $H\times H$ is switching the factors. In fact, this is a bijection onto the subset of $\mathrm{Hom}_\sigma(G, H\times H)$ that surject onto the first factor. Let $\mathcal{F}$ be the set of σ-invariant subgroups of $H\times H$ that surject onto the first factor. Then

$$|\mathrm{Sur}(G, H)| = \sum_{F\in\mathcal{F}} |\mathrm{Sur}_\sigma(G, F)|. \tag{3}$$

Note since σ is GI on G, if it is not *GI* on F, then $|\mathrm{Sur}_\sigma(G, F)| = 0$. Thus (3) would still hold if we restrict the sum on the right to F such that switching factors in $H\times H$ is *GI* on F (i.e. F generated by elements of the form (h, h^{-1}) for $h\in H$).

Acknowledgements

The authors thank Jordan Ellenberg, Daniel Ross and Akshay Venkatesh for helpful conversations. We thank Bjorn Poonen for pointing out a mistake in an earlier version of Lemma 4.7 as well as providing a quicker proof of the lemma. The first author was supported by Simons Foundation Award MSN-179747. The second author was supported by an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, and National Science Foundation grants DMS-1147782 and DMS-1301690.

References

AM15 M. Adam and G. Malle, *A class group heuristic based on the distribution of 1-eigenspaces in matrix groups*, J. Number Theory **149** (2015), 225–235.

Bha14 M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials*, Preprint (2014), arXiv:1402.0031.

Bos91 N. Boston, *Explicit deformation of Galois representations*, Invent. Math. **103** (1991), 181–196.

BBH16 N. Boston, M. Bush and F. Hajir, *Heuristics for p-class towers of imaginary quadratic fields*, Math. Ann. (2016), 1–37; doi:10.1007/s00208-016-1449-3.

BN06 N. Boston and H. Nover, *Computing pro-p Galois groups*, in *Algorithmic number theory, Proc. 7th int. symposium, ANTS-VII, Berlin, July 23–28, 2006* (Springer, 2006), 1–10.

CKLPW15 J. Clancy, N. Kaplan, T. Leake, S. Payne and M. M. Wood, *On a Cohen–Lenstra heuristic for Jacobians of random graphs*, J. Algebraic Combin. **42** (2015), 701–723.

CL84 H. Cohen and H. W. Lenstra Jr, *Heuristics on class groups of number fields*, in *Number theory, Noordwijkerhout 1983*, Lecture Notes in Mathematics, vol. 1068 (Springer, Berlin, 1984), 33–62.

EVW12 J. Ellenberg, A. Venkatesh and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen Lenstra conjecture over function fields, II*, Preprint (2012), arXiv:1212.0923.

EVW16 J. S. Ellenberg, A. Venkatesh and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), 729–786.

FW89 E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over a finite field*, in *Théorie des nombres, Quebec, 1987* (de Gruyter, Berlin, 1989), 227–239.

Gar15 D. Garton, *Random matrices, the Cohen–Lenstra heuristics, and roots of unity*, Algebra Number Theory **9** (2015), 149–171.

Gor07 D. Gorenstein, *Finite groups*, AMS Chelsea Publishing Series (American Mathematical Society, Providence, RI, 2007).

Gru76 K. W. Gruenberg, *Relation modules of finite groups*, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, vol. 25 (American Mathematical Society, Providence, RI, 1976).

HM01 F. Hajir and C. Maire, *Asymptotically good towers of global fields*, in *3rd European congress of mathematics (ECM), Vol. II, Barcelona, Spain, July 10–14, 2000*, Progress in Mathematics, vol. 202, eds C. Casacuberta *et al.* (Birkhäuser, Basel, 2001), 207–218.

Hal34 P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. Lond. Math. Soc. (2) **36** (1934), 29–95.

KV75 H. Koch and B. B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Astèrisque **24–25** (1975), 57–67.

Mal08 G. Malle, *Cohen–Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), 2823–2835.

O'B90 E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.

SGA4(3) M. Artin, A. Grothendieck and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 3, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4)*, Lecture Notes in Mathematics, vol. 305 (Springer, New York, NY, 1973); avec la collaboration de P. Deligne et B. Saint-Donat.

Wil98 J. S. Wilson, *Profinite groups* (Clarendon Press, Oxford, 1998).

Nigel Boston boston@math.wisc.edu
Department of Mathematics, University of Wisconsin-Madison,
480 Lincoln Drive, Madison, WI 53706, USA

Melanie Matchett Wood mmwood@math.wisc.edu
Department of Mathematics, University of Wisconsin-Madison,
480 Lincoln Drive, Madison, WI 53706, USA

and

American Institute of Mathematics, 600 East Brokaw Road,
San Jose, CA 95112, USA

https://doi.org/10.1112/S0010437X17007102 Published online by Cambridge University Press