PROBABILITY THEORY FOR RANDOM GROUPS ARISING IN NUMBER THEORY

MELANIE MATCHETT WOOD

ABSTRACT

We consider the probability theory, and in particular the moment problem and universality theorems, for random groups of the sort that arise or are conjectured to arise in number theory, and in related situations in topology and combinatorics. The distributions of random groups that are discussed include those conjectured in the Cohen–Lenstra–Martinet heuristics to be the distributions of class groups of random number fields, as well as distributions of nonabelian generalizations, and those conjectured to be the distributions of Selmer groups of random elliptic curves. For these sorts of distributions on finite and profinite groups, we survey what is known about the moment problem and universality, give a few new results including new applications, and suggest open problems.

MATHEMATICS SUBJECT CLASSIFICATION 2020

Primary 60E05; Secondary 60B99, 60F05, 15B52, 11R29, 11R45

KEYWORDS

Random groups, moment problem, universality, Cohen-Lenstra heuristics, arithmetic statistics, random matrices

INTERNATIONAL CONGRESS
OF MATHEMATICIANS
2022 JULY 6–14

Proc. Int. Cong. Math. 2022, Vol. 6, pp. 4476–4508
DOI 10.4171/ICM2022/145

1. INTRODUCTION

In this paper we will discuss the probability theory of random groups that arise in number theory and related areas, and the applications of that probability theory to other fields. We focus on the moment problem and on universality results for these random groups. While our focus is on the probability theory, we use potential applications in number theory, as well as topology and combinatorics, to motivate the kind of random groups on which we focus our probabilistic study.

One of the first motivating examples is the Cohen–Lenstra distribution on finite abelian p-groups. Let p be a prime and let X_{CL} be a random finite abelian p-group such that

$$\operatorname{Prob}(X_{\mathrm{CL}} \simeq A) = \frac{\prod_{i \geq 1}(1 - p^{-i})}{|\operatorname{Aut}(A)|}$$

for each finite abelian p-group A. For p an odd prime, let C_B be the Sylow p-subgroup of the class group of a uniform random imaginary quadratic field K with $|\operatorname{Disc} K| \leq B$. Then Cohen and Lenstra [15] conjectured that for each finite abelian p-group A,

$$\lim_{B \to \infty} \operatorname{Prob}(C_B \simeq A) = \operatorname{Prob}(X_{\mathrm{CL}} \simeq A), \tag{1.1}$$

i.e., that the C_B converge (in distribution) to X_{CL}. This X_{CL} is our starting example of a random group whose probability theory we wish to understand. Throughout the paper, we will consider more examples, including those related to generalizations of C_B such as when quadratic extensions are replaced by higher degree extensions or when the base field $\mathbb{Q}$ is replaced by another number field or $\mathbb{F}_q(t)$. We will consider nonabelian analogs where we consider $\operatorname{Gal}(K^{un}/K)$, the Galois group of the maximal unramified extension of K, in place of the class group. We will mention connections to analogous random groups arising in other fields, such as $\pi_1(M)$ or $H_1(M)$ for a random 3-manifold M, or the Jacobian (also known as sandpile group) of a random graph.

With these examples in mind, we first discuss the moment problem. Given a random variable X of a certain type, based on the type of random variable, we choose certain real-valued functions $f_0, f_1, \ldots$ and call the averages $\mathbb{E}(f_k(X))$ the *moments* of X. When X is real valued, we usually take $f_k(X) = X^k$, but when X is a random group we usually take $f_k(X)$ to be the number $\# \operatorname{Sur}(X, G_k)$ of surjective homomorphisms from X to a group G_k. The moment problem asks when the distribution of the random variable is determined uniquely from these moments. This is very useful in applications because the moments are usually easier to access than a distribution itself, and we will discuss many applications to class groups and their generalizations.

Next, we discuss universality questions in the sense of the central limit theorem. We ask when and how can we build a random group from many independent inputs such that in a limit the random group is insensitive to the distribution of the random inputs. When this happens, the output distribution is, of course, a natural one (as in the normal distribution in the Central Limit Theorem), and it tells us that such distributions are likely to arise in nature. This can help provide further motivation and context for conjectures in number theory. As the theory develops, we expect there will be further applications of these universality results to other fields.

For both topics, we will review what is known for random abelian and nonabelian groups, mention many applications, prove a few new results and applications, and suggest open problems.

1.1. Notation and conventions

We use $\mathbb{E}$ to denote the expectation of a real-valued random variable.

For a finite set S, we use $\#S$ or $|S|$ to denote the size of the set.

We write $\mathbb{F}_q$ for the finite field with q elements.

For a set of primes P, a P-group is a group whose order is a product of powers of primes in P, and a pro-P group is a profinite group all of whose continuous finite quotients are P-groups. The pro-P completion of a group is the inverse limit of all of its P-group quotients (and is a pro-P group).

We use Hom, resp. Sur, to denote homomorphisms, resp. surjective homomorphisms, always in the category of whatever the objects are in, e.g., for profinite groups we take continuous homomorphisms, and for R-modules we take R-module homomorphisms. Sometimes we use a subscript, e.g., $\mathrm{Sur}_R(A, B)$, as a reminder of the category. We use Aut to denote automorphisms with the same caveats.

When we take a random finite group, it is always with the discrete σ-algebra on the set of finite groups.

For random variables $Y, X_0, \dots$ with respect to a Borel σ-algebra, we say the X_n weakly converge in distribution to Y if for every open set U we have $\liminf \mathrm{Prob}(X_n \in U) \geq \mathrm{Prob}(Y \in U)$. By the Portmanteau theorem, this is equivalent to many other conditions. In this paper, in the topologies we consider, every open set is a countable disjoint union of basic open sets (used to define the topology), and each basic open set is also closed. In these settings, weak convergence in distribution is equivalent to having, for each basic open set U, $\lim_{n\to\infty} \mathrm{Prob}(X_n \in U) = \mathrm{Prob}(Y \in U)$ (see [33, PROOF OF THEOREM 1.1]).

For an abelian group A, we have $\wedge^2 A$ is the quotient of $A \otimes A$ by the subgroup generated by elements of the form $a \otimes a$ (and for an R-module A, we define $\wedge^2_R A$ similarly with the tensor product over R) and $\mathrm{Sym}^2 A$ is the quotient of $A \otimes A$ by the subgroup generated by elements of the form $a \otimes b - b \otimes a$.

For a group (resp. profinite group) G and elements $g_1, \dots \in G$, we write $\langle g_1, \dots \rangle$ for the normal subgroup (resp. closed normal subgroup) generated by $g_1, \dots$.

For a function $f(x)$, we write $f(x) = O(g(x))$ to mean that there exists a constant C such that for all x such that $f(x)$ is defined, we have $|f(x)| \leq Cg(x)$.

For a group G with an action of a group Γ, we write G^Γ for the invariants, i.e., elements of G that are fixed by every element of Γ.

In the distributions of interest from number theory, there will usually be a random number field, or random elliptic curve, or some such object behind the scenes. In these situations, there are a countable number of objects of interest (such as imaginary quadratic number fields), and we consider some enumeration of them such that there are a finite number up to some bound B, and then we take a uniform random object up to bound B, and consider the limit of these distributions as $B \to \infty$. We do not wish to suggest that the uniform distribution is the only distribution on a finite set. Indeed, the entire point of Section 3 is based on the fact that there are many nonuniform distributions. Even beyond the question of the distribution on the objects up to bound B, there is still a question of which enumeration one takes and this can have interesting and important effects (e.g., see [3, 45]). However, since we are using the examples from number theory mainly as motivation, in this paper we will usually be very brief or not mention at all how exactly we take the random number theoretic objects.

2. THE MOMENT PROBLEM

In probability, one often detects the distribution of a random variable by its moments, i.e., the averages of certain functions of the random variable. Most classically, the moments of a random variable $X \in \mathbb{R}$ are the averages $\mathbb{E}(X^k)$, indexed by natural numbers k, and the (mixed) moments of a random variable $(X_1, \dots, X_n) \in \mathbb{R}^n$ are the averages $\mathbb{E}(X_1^{k_1} \cdots X_n^{k_n})$, indexed by n-tuples of natural numbers $(k_1, \dots, k_n)$.

The moment problem asks whether moments determine a unique distribution, and results on the moment problem, such as the following, are foundational in probability theory.

Theorem 2.1 (Carleman's condition). *Let X be a random real number such that $M_k = \mathbb{E}(X^k)$ is finite for all integers $k \geq 0$. Then if*

$$\sum_{k \geq 1} M_{2k}^{-\frac{1}{2k}} = \infty, \tag{2.2}$$

then there is a unique distribution for a random real number Y such that $\mathbb{E}(Y^k) = M_k$ for all $k \geq 0$. In particular, if $M_k = O(e^k)$, then (2.2) holds.

This kind of uniqueness result is useful in a situation when we have a conjectural distribution, know its moments, and then can prove some random variable is distributed as conjectured by showing it has those moments. In other situations, we have an unknown distribution, compute its moments, and then recognize those as moments of a well-known distribution, and can use a uniqueness result to show our distribution matches the well-known one.

In many applications we have not a single random variable, but rather a sequence of random variables, and we seek their limiting distribution. For this, we require a uniqueness theorem that is *robust*, in the sense that we can prove that a sequence of random variables whose moments converge to certain values must converge in distribution to a certain limit.

Now we will clarify some, slightly informal, language to talk about different aspects of the moment problem. Suppose we are considering random variables taking values in some set, and a sequence of real-valued functions $f_0, f_1, f_2, \dots$ on that set whose averages give the moments of the random variables. We say we have *uniqueness* in the moment problem for moments $M_k \in \mathbb{R}$, if the following holds: for any two random variables X, Y under consideration, if for all k we have $\mathbb{E}(f_k(X)) = \mathbb{E}(f_k(Y)) = M_k$, then X and Y have the same distribution. We say we have *robust uniqueness* in the moment problem for moments $M_k \in \mathbb{R}$, if the following holds: for any sequence of random variables $Y, X_1, X_2, X_3, \ldots$ under consideration, if for all k we have $\lim_{n\to\infty} \mathbb{E}(f_k(X_n)) = \mathbb{E}(f_k(Y)) = M_k$, then the X_n weakly converge in distribution to Y. We have *existence* in the moment problem for moments $M_k \in \mathbb{R}$, if we know there exists a random variable X with $\mathbb{E}(f_k(X)) = M_k$ for all k, and we have *construction* in the moment problem for moments $M_k \in \mathbb{R}$ if we have existence and can moreover explicitly describe X by giving useful formulas for its distribution on enough subsets to generate the underlying σ-algebra.

2.1. Robust uniqueness for random abelian groups

For example, Fouvry and Klüners [21] determined the distribution of the 4-ranks $(2C_B)[2]$, where C_B is the 2-Sylow subgroup of the class group of a random imaginary quadratic field as in Section 1, as $B \to \infty$. Fouvry and Klüners proved the following result (which covers all aspects of the moment problem for certain average values).

Theorem 2.3 ([22, THEOREM 1]). *If p is a prime and $X_1, X_2, \ldots$ are random finite-dimensional $\mathbb{F}_p$-vector spaces such that for every integer $k \geq 0$, we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}\big(X_n, \mathbb{F}_p^k\big)\big) = 1,$$

then for each integer $r \geq 0$, we have

$$\lim_{n\to\infty} \operatorname{Prob}\big(X_n \simeq \mathbb{F}_p^r\big) = p^{-r^2} \frac{\prod_{j=r+1}^{\infty}(1-p^{-j})}{\prod_{j=1}^{r}(1-p^{-j})}.$$

The distribution and averages in Theorem 2.3 are known to occur as $\operatorname{Prob}(X_{\mathrm{CL}}/pX_{\mathrm{CL}} \simeq \mathbb{F}_p^r)$ and $\mathbb{E}(\#\operatorname{Sur}(X_{\mathrm{CL}}/pX_{\mathrm{CL}}, \mathbb{F}_p^k))$, respectively, for the random group X_{CL} introduced in Section 1 (see [15, THEOREM 6.3, COROLLARY 6.5]), so there does exist a random variable with these averages and its distribution can be explicitly described. In the paper [21], Fouvry and Klüners determined the averages $\mathbb{E}(\#\operatorname{Sur}((2C_B)[2], \mathbb{F}_2^k))$, and then applied Theorem 2.3 to determine the distribution of 4-ranks of class groups of imaginary quadratic fields (and did the analogous work for class groups of real quadratic fields).

Fouvry and Klüners actually write $\prod_{0\leq i<k}(p^{\operatorname{rk}_p(X_n)} - p^i)$, and we have interpreted that as the number of surjective homomorphisms $\#\operatorname{Sur}(X_n, \mathbb{F}_p^k)$. In [22], Fouvry and Klüners translate the knowledge of the averages of $\prod_{0\leq i<k}(p^{\operatorname{rk}_p(X)} - p^i)$ for all k to the knowledge of the averages of $p^{\operatorname{rk}_p(X)k} = \#\operatorname{Hom}(X, \mathbb{F}_p^k)$ for all k (which can be done by a finite sum over the subgroups of $\mathbb{F}_p^k$). These latter averages are the classical moments of the random number $p^{\operatorname{rk}_p(X)} = |X|$. When our random groups get more complicated (and in particular nonabelian), we will not be able to capture the entire data of our groups so simply in a number, or even a sequence of numbers, but the functions $\#\operatorname{Sur}(-, G)$ or $\#\operatorname{Hom}(-, G)$ will continue to be important and convenient functions whose averages we will call the moments (or Sur-moments, Hom-moments) of a random group. (See [13, SECTION 3.3] for a discussion about the fact that the Hom-moments for finite abelian p-groups are classical mixed moments of certain numerical invariants of the groups.) The relationship between the Hom-moments and the Sur-moments is analogous to the relationship of the moments $\mathbb{E}(X^k)$ and the factorial

moments $\mathbb{E}(X(X-1)\cdots(X-k+1))$ of a random real number—knowledge of either kind of moments for $k \leq m$ easily gives knowledge of the other kind for $k \leq m$, and the choice of which to use mainly depends which is more convenient for the problem at hand.

Fouvry and Klüners's proof of the robust uniqueness part of Theorem 2.3 actually works whenever

$$\mathbb{E}\big(\#\operatorname{Hom}(X, \mathbb{F}_p^k)\big) = \mathbb{E}\big(|X|^k\big) = O(p^{k^2/2})$$

(see [22, PROPOSITION 3]), echoing the refrain that moments that do not grow too quickly determine a distribution. (Note that in this generality we are not claiming existence of a distribution, but only uniqueness.) Such moments are too large to use Carleman's condition to conclude the distribution of $|X|$ as a real number, and indeed there are different distributions of real numbers that give the same moments with this order of growth (e.g., various distributions that have the same moments as the log-normal distribution). However, in our setting, of course, $|X|$ is restrained to be a power of p.

For a random cyclic cubic field K, with class group Cl_K with 3-torsion $\mathrm{Cl}_K[3]$, Klys [28] found the asymptotic moments of $\mathrm{Cl}_K[3]/\operatorname{Cl}_K[3]^{\mathrm{Gal}(K/\mathbb{Q})}$, and then applied the more general form of Theorem 2.3 to determine the limiting distribution of $\mathrm{Cl}_K[3]/\operatorname{Cl}_K[3]^{\mathrm{Gal}(K/\mathbb{Q})}$.

Ellenberg, Venkatesh, and Westerland prove the following.

Theorem 2.4 ([19, PROPOSITION 8.3]). *If for each $n \geq 0$, we have a random abelian p-groups X_n such that for every abelian p-group A we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}(X_n, A)\big) = 1,$$

then the X_n weakly converge in distribution to X_{CL}, i.e., for every abelian p-group B, we have

$$\lim_{n\to\infty} \operatorname{Prob}(X_n \simeq B) = \operatorname{Prob}(X_{\mathrm{CL}} \simeq B) = \frac{\prod_{i\geq 1}(1-p^{-i})}{|\operatorname{Aut}(B)|}.$$

Ellenberg, Venkatesh, and Westerland use Theorem 2.4, along with a determination of certain limiting moments of class groups of imaginary quadratic extensions of $\mathbb{F}_q(t)$, to prove that in a limit where the discriminant goes to infinity and then q goes to infinity, that the ℓ-Sylow subgroups of these class groups are as predicted by the Cohen–Lenstra heuristics for any odd prime ℓ, as long as $\ell \nmid q-1$ [19, THEOREM 1.2]. The work of Ellenberg, Venkatesh, and Westerland also particularly pioneered the idea that it is useful to consider these averages of surjection counts to be moments.

If we would like to consider more general finite abelian groups, and also distributions that have other moments, we have the following theorem by the author. (The cited results are stated with stronger bounds on the M_A, but one can see that all that is used in the proof is the hypotheses below.)

Theorem 2.5 (see [44, THEOREM 8.3, PROOF OF COROLLARY 9.2]). *Let P be a finite set of primes, and let $\mathcal{A}$ be the set of finite abelian P-groups. Let $M_A \in \mathbb{R}$ for each $A \in \mathcal{A}$ such that $M_A = O(|\wedge^2 A|)$. Let $Y, X_1, X_2, \ldots$ be random groups in $\mathcal{A}$. If for every $A \in \mathcal{A}$, we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}(X_n, A)\big) = \mathbb{E}\big(\#\operatorname{Sur}(Y, A)\big) = M_A,$$

then the X_n weakly converge in distribution to Y, i.e., for every $B \in \mathcal{A}$,

$$\lim_{n\to\infty} \operatorname{Prob}(X_n \simeq B) = \operatorname{Prob}(Y \simeq B).$$

When $A = \mathbb{F}_p^k$, we have $|\wedge^2 A| = p^{k(k-1)/2}$, so we see a similar upper bound to that of Fouvry and Klüners. Theorem 2.5 was applied in [44] to determine the limiting distribution of the Jacobians (also known as sandpile groups) of Erdős–Rényi random graphs, and by Mészáros [37] to determine the limiting distribution of the Jacobians of random regular graphs. Mészáros's result then had the striking corollary that the adjacency matrix of a random regular graph is invertible with high probability, answering a long-standing open question that is not a priori about random groups at all.

If we consider a random finite abelian group X, without any condition on primes dividing its order, we have a uniqueness result by W. Wang and the author as a corollary of Theorem 2.5.

Corollary 2.6 ([43, THEOREM 6.13]). *Let $M_A \in \mathbb{R}$ for each finite abelian group A such that $M_A = O(|\wedge^2 A|)$. Let X, Y be random finite abelian groups. If for every finite abelian group A, we have*

$$\mathbb{E}\big(\#\operatorname{Sur}(X, A)\big) = \mathbb{E}\big(\#\operatorname{Sur}(Y, A)\big) = M_A,$$

then X and Y have the same distribution, i.e., for every finite abelian group B,

$$\operatorname{Prob}(X \simeq B) = \operatorname{Prob}(Y \simeq B).$$

Proof. For a finite abelian group C, let C_p denote its Sylow p-subgroup. We have

$$\operatorname{Prob}(X \simeq A) = \lim_{z\to\infty} \operatorname{Prob}\bigg(\prod_{p\le z} X_p \simeq \prod_{p\le z} A_p\bigg).$$

Then we can apply Theorem 2.5 with P the set of primes at most z to conclude the corollary. ∎

However, for general finite abelian groups, robustness no longer holds (as it is possible the limit in n cannot be exchanged with the limit in z). As in [43, EXAMPLE 6.14], we can consider a random finite abelian group X, e.g., such that

$$\operatorname{Prob}(X \simeq A) = \frac{\zeta(2)^{-1}\zeta(3)^{-1}\zeta(4)^{-1}\cdots}{|A||\operatorname{Aut} A|},$$

where ζ is the Riemann zeta function and we can also write $\zeta(2)^{-1}\zeta(3)^{-1}\zeta(4)^{-1}\cdots$ as a product over primes $\prod_p \prod_{i\ge2}(1-p^{-i})$. (There is a random group with this distribution–see e.g., [46, PROPOSITION 2.1], and it is the limiting distribution predicted by Gerth's extension [25] of the Cohen–Lenstra heuristics for $2\operatorname{Cl}_K$, where K is a random real quadratic field.) Then consider the random groups $X \times \mathbb{Z}/p\mathbb{Z}$ for each prime p. For any finite abelian group A, we have $\lim_{p\to\infty} \mathbb{E}(\#\operatorname{Sur}(X \times \mathbb{Z}/p\mathbb{Z}, A)) = \mathbb{E}(\#\operatorname{Sur}(X, A))$ since for p large enough $p \nmid |A|$. Yet the limiting distribution of the $X \times \mathbb{Z}/p\mathbb{Z}$ is the zero distribution, i.e., for each A we have $\lim_{p\to\infty} \operatorname{Prob}(X \times \mathbb{Z}/p\mathbb{Z} \simeq A) = 0$. This is in stark contrast to the situation for random real numbers [7, THEOREM 30.2], where whenever the moments determine a unique distribution, they do so robustly.

2.2. When uniqueness fails

Another important example of distributions arising in number theory are those predicted by Poonen and Rains [39] as the asymptotic distributions of p-Selmer groups of random elliptic curves. We consider two different random $\mathbb{F}_p$ vector spaces, with distributions given as follows:

$$\begin{aligned}\operatorname{Prob}\big(X_{\mathrm{odd}} \simeq \mathbb{F}_p^k\big) &= \begin{cases} p^{-(k^2-k)/2}\frac{\prod_{j=0}^{\infty}(1-p^{-2j-1})}{\prod_{j=1}^{k}(1-p^{-j})} & k \text{ odd},\\ 0 & k \text{ even},\end{cases}\\ \operatorname{Prob}\big(X_{\mathrm{even}} \simeq \mathbb{F}_p^k\big) &= \begin{cases} p^{-(k^2-k)/2}\frac{\prod_{j=0}^{\infty}(1-p^{-2j-1})}{\prod_{j=1}^{k}(1-p^{-j})} & k \text{ even},\\ 0 & k \text{ odd}.\end{cases}\end{aligned} \tag{2.7}$$

Poonen and Rains [39] conjecture that these are the limiting distributions of p-Selmer group of elliptic curves over $\mathbb{Q}$ of odd and even parity, respectively, and note [39, PROPOSITION 2.22(C)] that these distributions have the same moments, even though they are quite different distributions, supported on entirely disjoint sets of groups. Indeed, there moments are as follows, and we see that these cases are just beyond the bounds of the uniqueness results mentioned above.

Theorem 2.8. *For each $k \geq 0$, we have*

$$\mathbb{E}\big(\#\operatorname{Sur}\big(X_{\mathrm{odd}}, \mathbb{F}_p^k\big)\big) = \mathbb{E}\big(\#\operatorname{Sur}\big(X_{\mathrm{even}}, \mathbb{F}_p^k\big)\big) = p^{(k^2+k)/2}, \quad \textit{and}$$
$$\mathbb{E}\big(\#\operatorname{Hom}\big(X_{\mathrm{odd}}, \mathbb{F}_p^k\big)\big) = \mathbb{E}\big(\#\operatorname{Hom}\big(X_{\mathrm{even}}, \mathbb{F}_p^k\big)\big) = p^{(k^2+k)/2}\prod_{j=1}^{k}\big(1+p^{-j}\big).$$

Proof sketch. The Hom-moments are shown in [39, PROPOSITION 2.22(C)]. The Sur-moments can be found, in principle, by applying Möbius inversion to the Hom-moments. However, the following argument is perhaps more practical. The distributions of X_{odd} and X_{even} occur as the limiting distribution of cokernels of uniform random $n \times n$ alternating matrices over $\mathbb{F}_p$ (where n is odd or even, respectively). It is a general feature that for various computations it can be helpful, even for a known distribution, to recognize it as the limit of natural distributions. We can see the claimed limit by counting exactly how many alternating matrices over $\mathbb{F}_p$ have corank k for each k as in [31, PROPOSITION 3.8] (see also [5, THEOREM 1.10]). Then, one can make a simple argument to compute the limiting moments of these random cokernels as in [13, THEOREM 11] (which does the analogous thing for symmetric matrices), and use the explicit formulas for the distribution of the random cokernels for each k and n along with the dominated convergence theorem, as in [13, THEOREM 10], to deduce that the limiting moments of the random cokernels agree with the moments of X_{odd} and X_{even}. ■

However, in a setting as we have described, we could also use the additional information that we are looking for a distribution supported only on groups of even rank (or odd rank), along with the moments, to determine a distribution.

One important motivation for the conjectures of Poonen and Rains was the result of Heath-Brown [26] determining the limiting distribution of 2-Selmer groups of a random quadratic twist of the congruent number curve. Heath-Brown showed that the limiting distribution for the quotient of the 2-Selmer group by the $\mathbb{F}_2^2$ coming from the 2-torsion points on the curve is the X_{odd} distribution for twists $D \equiv 5, 7 \pmod 8$ (when the Selmer rank is odd), and the X_{even} distribution for twists $D \equiv 1, 3 \pmod 8$ (when the Selmer rank is even). Heath-Brown determined these distributions by first determining the moments and then proving a robust uniqueness result for the moment problem. Heath-Brown pointed out that it was surprising that these different distributions had the same moment, and proved the following robust uniqueness result, taking into account the parity.

Theorem 2.9 ([26, LEMMA 18, PROOF OF THEOREM 2]). *Let $M_0, M_2, \ldots$ be nonnegative real numbers such that $M_k = O(2^{k(k+1)/2})$. Let $Y, X_1, X_2, \ldots$ be random even dimensional $\mathbb{F}_2$-vector spaces. Then if for every even $k \geq 0$, we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Hom}(X_n, \mathbb{F}_2^k)\big) = \mathbb{E}\big(\#\operatorname{Hom}(Y, \mathbb{F}_2^k)\big) = M_k,$$

then the X_n weakly converge in distribution to Y, i.e., for every even r, we have

$$\lim_{n\to\infty} \operatorname{Prob}\big(X_n \simeq \mathbb{F}_2^r\big) = \operatorname{Prob}\big(Y \simeq \mathbb{F}_2^r\big).$$

The statement also holds if we replace "even" with "odd."

Feng, Landesman, and Rains [20] face a similar issue (in a slightly different context, where the random groups have fixed finite support of a given parity, but they only know half the moments) and use knowledge of the parity along with moments to determine the distribution of n-Selmer groups of elliptic curves of fixed height over $\mathbb{F}_q(t)$ as $q \to \infty$.

Given the two distributions of X_{odd} and X_{even} on $\mathbb{F}_p$-vector spaces given in (2.7), one natural question is what are all the distributions on $\mathbb{F}_p$-vector spaces with those same moments. We will now show that these (plus their linear combinations) are the only such distributions.

Theorem 2.10. *Given nonnegative reals $M_{-1}, M_0, M_1, \ldots,$ and $p > 1$, and $b < 3$, such that $M_k = O(p^{\frac{k^2+bk}{2}})$, there is at most one simultaneous solution $(x_s)_s$ to*

$$\sum_{s=0}^{\infty} (-1)^s x_s = M_{-1} \quad \textit{and}$$

$$\sum_{s=0}^{\infty} x_s p^{sk} = M_k, \quad k = 0, 1, \ldots,$$

such that $x_s \geq 0$ for all s.

We note that this proof strategy is in the style of the earliest work on this problem, and not the more recent work, but it will also let us see some of the main features of the moment problem.

Proof. We modify the method from [26, LEMMA 18]. First, assuming we have a nonnegative solution, we can bound x_s using the $k = s$ equation to obtain

$$x_s = O\big(p^{\frac{-s^2+bs}{2}}\big).$$

From this it follows that for any $N \geq 0$ and $k \leq N-2$,

$$\sum_{s \geq N} x_s p^{sk} = O\Big(\sum_{s \geq N} p^{\frac{-s^2+bs+2ks}{2}}\Big) = O\big(p^{\frac{-N^2+bN+2kN}{2}}\big),$$

where we allow the constant in the O to depend on p.

We take some positive integer N, and we truncate the system to write

$$\sum_{s=0}^{N-1} x_s p^{sk} = M'_k$$

for $k = -1, 0, 1, \dots, N-2$ (except for $k = -1$ we replace p^{sk} with $(-1)^s$). Let V be the $N \times N$ matrix whose i, j coefficient is $p^{(i-2)(j-1)}$ for $i \geq 2$ and $(-1)^{j-1}$ for $i = 1$. Let x be the vector with entries $x_0, \dots, x_{N-1}$ and M' the vector with entries $M'_{-1}, \dots, M'_{N-2}$. Then $Vx = M'$. (All of these implicitly depend on N.) We will just give the first row of V^{-1} explicitly. Since V is Vandermonde, we have $\det V = \prod_{0 \leq i < j \leq N-2}(p^j - p^i)\prod_{i=0}^{N-2}(p^i + 1)$. Note that the $(i, 1)$ minor of V is also Vandermonde (after dividing out a factor from each row) on the same elements, except for p^{i-2}, (or -1 when $i = 1$). So we have

$$\big(V^{-1}\big)_{1,j} = \frac{\pm p^{\frac{(N-2)(N-1)}{2} - (j-2)}}{(p^{j-2}+1)\prod_{\substack{0 \leq i \leq N-2 \\ i \neq j-2}}(p^{j-2} - p^i)} \tag{2.11}$$

for $j > 1$, and

$$\big(V^{-1}\big)_{1,1} = \frac{\pm p^{\frac{(N-2)(N-1)}{2}}}{\prod_{i=0}^{N-2}(p^i + 1)},$$

and in all cases

$$\big(V^{-1}\big)_{1,j} = O\big(p^{\frac{-j^2+j}{2}}\big).$$

So

$$\begin{aligned} x_0 &= \sum_{j=1}^{N} \big(V^{-1}\big)_{1,j} M'_{j-2} \\ &= \sum_{j=1}^{N} \big(V^{-1}\big)_{1,j} M_{j-2} + O\Bigg(\sum_{j=1}^{N} p^{\frac{-j^2+j}{2}} \big|M_{j-2} - M'_{j-2}\big|\Bigg) \\ &= \sum_{j=1}^{N} \big(V^{-1}\big)_{1,j} M_{j-2} + O\big(p^{\frac{(b-3)N}{2}}\big), \end{aligned}$$

meaning that x_0 must be $\lim_{N\to\infty} \sum_{j=1}^{N}(V^{-1})_{1,j} M_{j-2}$ (where the matrix V implicitly depends on N).

Once x_0 is determined, we notice that our equations imply

$$\sum_{s=1}^{\infty}(-1)^{s-1} x_s = -(M_{-1} - x_0) \quad \text{and}$$
$$\sum_{s=1}^{\infty} x_s p^{(s-1)k} = (M_k - x_0)p^{-k},$$

and we have a new system whose constants are still $O(p^{\frac{k^2+bk}{2}})$, and thus we can apply to same reasoning to deduce $x_1, \dots,$ each have at most 1 possible value. ■

Corollary 2.12. *If $\mu_{\mathrm{odd}}, \mu_{\mathrm{even}}$ are the distributions of $X_{\mathrm{odd}}, X_{\mathrm{even}}$, then any random $\mathbb{F}_p$-vector space X such that for all k,*

$$\mathbb{E}\big(\#\operatorname{Hom}\big(X, \mathbb{F}_p^k\big)\big) = p^{(k^2+k)/2} \prod_{j=1}^{k} \big(1 + p^{-j}\big)$$

has distribution $\lambda\mu_{\mathrm{odd}} + (1-\lambda)\mu_{\mathrm{even}}$ for some $0 \le \lambda \le 1$.

Proof. Clearly, $\lambda\mu_{\mathrm{odd}} + (1-\lambda)\mu_{\mathrm{even}}$ give distributions with these same moments, and they each assign a different probability to the group being odd rank. Let λ be the probability that X has odd rank. We apply Theorem 2.10 with $x_s = \operatorname{Prob}(X \simeq \mathbb{F}_p^s)$, and $M_{-1} = 1 - 2\lambda$, and $M_k = p^{(k^2+k)/2} \prod_{j=1}^{k}(1 + p^{-j})$, and find that there are unique values x_s satisfying the equations, which proves the corollary. ■

Open Problem 2.13. Besides the parity of the rank, are there other natural moments that we can consider for random finite $\mathbb{F}_p$-vector spaces, or finite abelian groups more generally, so that with the additional moments we can strengthen uniqueness results to allow for larger growing moments?

In forthcoming work of Nguyen and the author, we prove a generalization of the robust uniqueness result of Theorem 2.9 for random finite abelian groups whose orders are supported on a finite set of primes, with a parity condition on the group.

Theorem 2.14 (Nguyen–Wood, forthcoming). *Let P be a finite set of primes, and let $\mathcal{A}$ be the set of finite abelian P-groups. Let $M_A \in \mathbb{R}$ for each $A \in \mathcal{A}$ such that $M_A = O(|\operatorname{Sym}^2 A|)$. Let a be an integer and $Y, X_1, X_2, \dots$ be random groups in $\mathcal{A}$, either*

(1) *all supported on groups of the form $G \times G$, or*

(2) *all supported on groups of the form $\mathbb{Z}/a\mathbb{Z} \times G \times G$, for G with $aG = 0$.*

If for every $A \in \mathcal{A}$, we have

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}(X_n, A)\big) = \mathbb{E}\big(\#\operatorname{Sur}(Y, G)\big) = M_A,$$

then the X_n weakly converge in distribution to Y, i.e., for every $B \in \mathcal{A}$,

$$\lim_{n\to\infty} \operatorname{Prob}(X_n \simeq B) = \operatorname{Prob}(Y \simeq B).$$

2.3. Random finite abelian groups with additional structure

The class groups of Galois fields are not just abelian groups, but are also $\mathbb{Z}[G]$-modules, where G is the Galois group. Let $\mathbb{Z}[G]' = \mathbb{Z}[G, |G|^{-1}]$. Given a number field k and a finite group G, the Cohen–Lenstra–Martinet heuristics [15, 16] give a distribution on $\mathbb{Z}[G]'$-modules, and conjecture that a random G-extension of k has class group who prime-to-$|G|$ part is according to their distribution. Thus for potential number theoretic applications, one would like robust uniqueness for the moment problem for random finite $\mathbb{Z}[G]'$-modules. W. Wang and the author have given such a robust uniqueness result (the stated results are only for particular moments that occur in the Cohen–Lenstra–Martinet heuristics, but the proof works without change for the result given here).

Theorem 2.15 (See [43, THEOREM 6.11]). *Let G be a finite group. Let P be a finite set of primes, none dividing $|G|$, and let $\mathcal{A}$ be the set of finite P-group $\mathbb{Z}[G]'$-modules. Let $M_A \in \mathbb{R}$ for each $A \in \mathcal{A}$ such that $M_A = O(|\wedge^2_{\mathbb{Z}[G]'} A|)$. Let $Y, X_1, X_2, \dots$ be random $\mathbb{Z}[G]'$-modules in $\mathcal{A}$. If for every $A \in \mathcal{A}$, we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}_G(X_n, A)\big) = \mathbb{E}\big(\#\operatorname{Sur}_G(Y, A)\big) = M_A,$$

then the X_n weakly converge in distribution to Y, i.e., for every $B \in \mathcal{A}$,

$$\lim_{n\to\infty} \operatorname{Prob}(X_n \simeq B) = \operatorname{Prob}(Y \simeq B).$$

Theorem 2.15 can be applied to work of Liu, Zureick-Brown, and the author [34], to prove, for every finite group G, a function field analog of the Cohen–Lenstra–Martinet heuristics for G-extensions over $\mathbb{F}_q(t)$, as $q \to \infty$, as we will see below. Wang and the author [43, THEOREM 6.2] have found the moments of the Cohen–Lenstra–Martinet distributions on $\mathbb{Z}[G]'$-modules. In [34], we count and compare components of various Hurwitz schemes to estimate the moments of the class groups of random G-extensions of $\mathbb{F}_q(t)$, and notice those moments, in the limit where $q \to \infty$ and then the degree n of the (reduced) branch locus of the cover (i.e., the size of the radical of the discriminant) goes to infinity, match those predicted by Cohen–Lenstra–Martinet. Theorem 2.15 then tells us that the limiting distribution of these class groups, when q and n both go to ∞, and q is sufficiently large in terms of n, is as predicted by the Cohen–Lenstra–Martinet heuristics. (Some caveats: these results are only in the case of extensions split completely over infinity, are only about the part of the class group that is prime to $|G|$, and q must be taken so that $q-1$ is relatively prime to all the primes in P, and q is prime to $|G|$ and the primes in P. So these results do not see the part of the class group that is affected by roots of unity in $\mathbb{F}_q(t)$ [24, 36].) Precisely, we have the following.

Theorem 2.16 (Corollary of [34, COROLLARY 1.5] and [43, THEOREMS 6.2 AND 6.11]). *Let G be a finite group and P be a finite set of primes that are relatively prime to $|G|$. Let B be a finite abelian P-group $\mathbb{Z}[G]$-module, and $B^G = 0$.*

Let $K_{q,n}$ be a uniform random Galois G-extension K of $\mathbb{F}_q(t)$, split completely over ∞, with the norm of the radical of its discriminant $K/\mathbb{F}_q(t)$ at most q^n. Let $X_{q,n}$ be the product of the Sylow p-subgroups of the class group of $K_{q,n}$ (more precisely, of its ring of integers over $\mathbb{F}_q[t]$) for $p \in P$.

Then if q_n is a sequence of prime powers growing sufficiently fast in n, such that for all n we have that q_n is relatively prime to $|G|$ and all the primes in P and $q_n - 1$ is relatively prime to all the primes in P, then

$$\lim_{n\to\infty} \operatorname{Prob}(X_{q_n,n} \simeq B) = \frac{c}{|B||\operatorname{Aut}_G(B)|},$$

where c is a constant depending on G and P such that the limiting probabilities above sum, over B, to 1.

Proof. By [34, COROLLARY 1.5], for every finite abelian P-group $\mathbb{Z}[G]$-module H with $H^G = 0$, and every $\epsilon > 0$, there is an N_ϵ, such that for $n \geq N_\epsilon$, we have

$$\left| \lim_{\substack{q\to\infty \\ (q,|G|)=1 \\ (q(q-1),p)=1 \text{ for } p\in P}} \mathbb{E}\big(\#\operatorname{Sur}_G(X_{q,n}, H)\big) - |H|^{-1} \right| \leq \epsilon/2.$$

For $n \geq N_\epsilon$, we choose a $Q_{n,\epsilon}$ such that for $q \geq Q_{n,\epsilon}$ (satisfying the conditions above) we have

$$\left|\mathbb{E}\big(\#\operatorname{Sur}_G(X_{q,n}, H)\big) - |H|^{-1}\right| \leq \epsilon.$$

So, if for each n, we consider the smallest ϵ such that $n \geq N_\epsilon$, and then take $q_n \geq Q_{n,\epsilon}$, we have

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}_G(X_{q_n,n}, H)\big) = |H|^{-1}.$$

Since $\operatorname{Cl}\mathcal{O}_K$ is trivial and $(|X_{q,n}|, |G|) = 1$, we have $X_{q,n}^G = 0$ [16, COROLLARY 7.7], so if H is such that $H^G \neq 0$, we have $\#\operatorname{Sur}_G(X_{q,n}, H) = 0$. By [43, THEOREM 6.2], we have that these are also the moments of the random $\mathbb{Z}[G]$-module Y such that for any finite abelian P-group $\mathbb{Z}[G]$-module B with $B^G = 0$ (on which Y is supported)

$$\operatorname{Prob}(Y \simeq B) = \frac{c}{|B||\operatorname{Aut}_G(B)|},$$

where c is a constant depending only on P and G. Thus by Theorem 2.15 we conclude the theorem. ■

As described by Wang and the author [43, SECTIONS 7–8], the class groups of non-Galois fields, away from certain bad primes, are also modules for a certain maximal order $\mathfrak{o}$ in a semisimple algebra depending on the Galois group G of the Galois closure over $\mathbb{Q}$ and over the field itself, and moreover are determined (as modules) from the class group of the Galois closure. The algebra $\mathfrak{o}$ can be nontrivial even when the non-Galois field has no automorphism. We can thus show that the Cohen–Lenstra–Martinet heuristics imply conjectures for the distribution of class groups of non-Galois fields. For the part of the class group prime to $|G|$, analogous results to Theorem 2.16 for the non-Galois case then follow formally from Theorem 2.16 and the results in [43]. However, for non-Galois extensions, the "bad" primes avoided by the conjectures are not always all primes dividing $|G|$. So at certain "good" primes p dividing $|G|$, we have shown in [43, THEOREM 8.14] that the Cohen–Lenstra–Martinet heuristics imply a conjectural distribution on the Sylow p-subgroups of class groups of non-Galois extensions (with Galois closure of group G) as well. See [43, THEOREM 8.14] for the relevant notion of good primes. Here we mention a few examples of good primes: 2 for S_3 cubic extensions, 3 for A_4 and S_4 quartic extensions, 2 for quintic D_5 or A_5 extensions. The moment calculations and the unique robustness of the moment problem results in [43] include the situations for all good primes for non-Galois extensions, as they are more generally for distributions of modules over maximal orders in semisimple algebras.

In particular, the robust uniqueness result in [43, THEOREM 6.11] is a version of Theorem 2.5 in which $\mathbb{Z}[G]'$ is replaced by a maximal order in a semisimple algebra. Sawin [41, THEOREM 1.3] has proven a version of Theorem 2.5, in which $\mathbb{Z}[G]'$ is replaced by any associative algebra R such that there are only finitely many isomorphism classes of finite simple R-modules, and Ext^1_R between any two finite R-modules is finite, but one requires the stronger assumption that $M_A = O(|A|^{O(1)})$.

As another example of additional structure, for the Sylow p-subgroups of class groups of quadratic extensions of $\mathbb{F}_q(t)$, Lipnowski, Sawin, and Tsimerman find that these groups have additional structure when $p^n \mid q-1$ [32] (where $q-1$ crucially is the number of roots of unity in $\mathbb{F}_q(t)$). This structure involves two pairings and a compatibility relation, and they call a group with such structure a p^n-Bilinearly Enhanced Group. In [32, SECTION 8], they define moments for these enhanced groups and address the uniqueness and robustness aspects of the moments problem in this context. They then apply their moment problem result, along with the homological stability results of Ellenberg, Venkatesh, and Westerland [19], to give a limiting distribution of Sylow p-subgroups of class groups of quadratic extensions of $\mathbb{F}_q(t)$, along with this extra structure.

2.4. Random nonabelian groups

One can also consider random nonabelian groups. A natural such group arising in number theory is $\mathrm{Gal}(K^{un}/K)$, the Galois group of the maximal unramified extension of some random number field K. We have that $\mathrm{Gal}(K^{un}/K) = \pi_1^{\acute{e}t}(\mathrm{Spec}\,\mathcal{O}_K)$ and this group has abelianization Cl_K. The maximal pro-p quotient $G_p(K)$ of $\mathrm{Gal}(K^{un}/K)$ is the p-class tower group of K, the Galois group of K^p, the p-class tower of K.

Boston, Bush, and Hajir [9,10], inspired by the Cohen–Lenstra heuristics, developed heuristics predicting the distribution of $G_p(K)$ for K a random imaginary (respectively, real) quadratic field and p an odd prime. Boston and the author [11] found the moments of the conjectural distribution of Boston–Bush–Hajir for imaginary quadratic fields, and prove robust uniqueness for the moment problem for these moments.

Now, as we are considering random profinite groups, the set of isomorphism classes of groups under consideration is uncountable, and we need to be more precise about the measure theory. For a quadratic field K, note that $G_p(K)$ has an action of $\mathbb{Z}/2\mathbb{Z} = \mathrm{Gal}(K/\mathbb{Q})$, by lifting elements to $\mathrm{Gal}(K^p/\mathbb{Q})$ and conjugating. In general, this would only be an outer action, but since p is odd, by the Schur–Zassenhaus theorem we can find a splitting of $\mathrm{Gal}(K^p/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$, and the resulting action of $\mathrm{Gal}(K/\mathbb{Q})$ on $G_p(K)$ does not depend, up to isomorphism, on the choice of splitting. Let $\mathcal{G}_p$ be the set of isomorphism classes of finitely generated pro-p groups with a continuous action of $\mathbb{Z}/2\mathbb{Z}$ (i.e., where morphisms must be equivariant for the $\mathbb{Z}/2\mathbb{Z}$ action). A pro-p group has a canonical lower p-central series defined by $P_0(G) := G$, and for $n \geq 0$, we define $P_{n+1}(G)$ to be the closed subgroup generated by the commutators $[G, P_n(G)]$ and $P_n(G)^p$. A finitely generated pro-p group G then has canonical finite quotients $Q_n(G) := G/P_n(G)$. We let Ω be the σ-algebra on $\mathcal{G}_p$ generated by the sets

$$\{G \mid Q_c(G) \simeq P\},$$

as P ranges over p-groups. We consider all random variables valued in $\mathcal{G}_p$ to be for the σ-algebra Ω. (See [11, SECTION 3] for more details.) With these preliminaries, we can state the uniqueness result of Boston and the author.

Theorem 2.17 ([11, THEOREMS 1.3 AND 1.4]). *Let p be an odd prime. There is a random $X_{\mathrm{BBH}} \in \mathcal{G}_p$ whose distribution is the predicted distribution of Boston–Bush–Hajir for $G_p(K)$ for imaginary quadratic K. For all finite $P \in \mathcal{G}_p$, we have*

$$\mathbb{E}\big(\#\operatorname{Sur}_{\mathbb{Z}/2\mathbb{Z}}(X_{\mathrm{BBH}}, P)\big) = 1.$$

If we have a random $X \in \mathcal{G}_p$ such that, for all finite $P \in \mathcal{G}_p$, we have

$$\mathbb{E}\big(\#\operatorname{Sur}_{\mathbb{Z}/2\mathbb{Z}}(X, P)\big) = 1,$$

then X has the same distribution as X_{BBH}.

The argument in [11] actually shows the following more general uniqueness result.

Theorem 2.18 (see [11, LEMMA 4.7, PROOF OF THEOREM 4.9]). *Let p be a prime and $M_P \in \mathbb{R}$ for each finite $P \in \mathcal{G}_p$. Let $\mathcal{G}_p^c$ the image of $\mathcal{G}_p$ under Q_c. Suppose that for each $c \geq 0$ and each $P \in \mathcal{G}_p^c$, we have*

$$\sum_{Q \in \mathcal{G}_p^c} \frac{M_Q |\operatorname{Sur}_{\mathbb{Z}/2\mathbb{Z}}(Q, P)|}{M_P |\operatorname{Aut}_{\mathbb{Z}/2\mathbb{Z}}(Q)|} < 2. \tag{2.19}$$

If we have random $X, Y \in \mathcal{G}_p$ such that, for all finite $P \in \mathcal{G}_p$, we have

$$\mathbb{E}\big(\#\operatorname{Sur}_{\mathbb{Z}/2\mathbb{Z}}(X, P)\big) = \mathbb{E}\big(\#\operatorname{Sur}_{\mathbb{Z}/2\mathbb{Z}}(Y, P)\big) = M_P,$$

then X and Y have the same distribution.

The challenge in applying Theorem 2.18 is that it is not at all clear how one can evaluate the sum in (2.19). Note that (2.19) is a sum of quite a different flavor than if we were considering abelian groups. In particular, we do not have any convenient enumeration of all finite p-groups, and so evaluating this sum seems to involve a rather difficult group theory problem. In [11], we prove that (2.19) holds when p is odd and all M_P are 1, but by a round-about argument that uses the construction of X_{BBH}.

In [11], we analyze components of certain Hurwitz schemes to prove that in a certain function field analog some of the moments of $G_p(K)$ for quadratic $K/\mathbb{F}_q(t)$ (ramified at infinity) agree with the conjectures of Boston, Bush, and Hajir. In our result [11, THEOREM 1.5], we let the degree of the discriminant go to infinity, and then let q go to infinity, and as in Theorem 2.16 we require that $(q, 2p) = 1$ and $(q-1, p) = 1$. This result involves the generally more difficult limit of letting q go to infinity after the bound on the discriminant, as in the theorem of [19], and we also use the theorem of Ellenberg, Venkatesh, and Westerland [19] on the homological stability of Hurwitz spaces in the proof.

While Theorem 2.17 certainly helps contextualize the result of [11] on function field moments, it does not immediately apply because Theorem 2.17 proves only uniqueness and not robust uniqueness, which would be required in our desired applications, as they involve limits of distributions. In the nonabelian setting, Sawin recently proved a robust uniqueness result however that can be applied.

We will now explain what is required for this robust uniqueness result for nonabelian profinite groups. Fix a finite group Γ, and consider the set $\mathcal{G}$ of isomorphism classes of profinite groups with a continuous action of Γ, finitely many surjections to any finite group, and all continuous finite quotients of order relatively prime to $|\Gamma|$. We will define a topology on $\mathcal{G}$, introduced by Liu, Zureick-Brown, and the author [34] (based on [33]), and our σ-algebra Ω will be the Borel σ-algebra for that topology. As we used $Q_c(G)$ above, we would like our topology to filter our profinite groups by certain canonical finite quotients. We will make such a canonical finite quotient for any finite set $\mathcal{C}$ of finite groups with an action of Γ (we call these Γ-*groups*). Let $\bar{\mathcal{C}}$ be the closure of $\mathcal{C}$ under taking Γ-equivariant subgroups, products, and quotients. Let $G^{\mathcal{C}}$ be the inverse limit of all quotients of G that are in $\bar{\mathcal{C}}$. Then these $G^{\mathcal{C}}$ (indexed by finite sets $\mathcal{C}$ of finite groups) are the canonical quotients we will use. We then use the topology on $\mathcal{G}$ whose open sets are generated by

$$\{G \mid G^{\mathcal{C}} \simeq H\},$$

where H ranges over all finite Γ-groups. Then Sawin's robust uniqueness result can be stated as follows.

Theorem 2.20 ([41, THEOREM 1.2]). *Let Γ be a finite group and $\mathcal{C}$ be a finite set of finite Γ-groups whose orders are relatively prime to $|\Gamma|$. For every finite Γ-group H, let $M_H \in \mathbb{R}$ such that $M_H = O(|H|^{O(1)})$. Let $Y, X_1, X_2, \ldots$ be random groups in $\mathcal{G}$. Assume that for every finite Γ-group H with $H^{\mathcal{C}} = H$, we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}_\Gamma(X_n, H)\big) = \mathbb{E}\big(\#\operatorname{Sur}_\Gamma(Y, H)\big).$$

Then for every finite group H with an action of Γ,

$$\lim_{n\to\infty} \operatorname{Prob}(X_n^{\mathcal{C}} \simeq H) = \operatorname{Prob}(Y^{\mathcal{C}} \simeq H). \tag{2.21}$$

Corollary 2.22. *Let Γ be a finite group. For every finite Γ-group H, let $M_H \in \mathbb{R}$ such that $M_H = O(|H|^{O(1)})$. Let $Y, X_1, X_2, \ldots$ be random groups in $\mathcal{G}$. Assume that for every finite Γ-group H, we have*

$$\lim_{n\to\infty} \mathbb{E}\big(\#\operatorname{Sur}_\Gamma(X_n, H)\big) = \mathbb{E}\big(\#\operatorname{Sur}_\Gamma(Y, H)\big).$$

Then the distributions of the X_i weakly converge to the distribution of Y.

Sawin proved Theorem 2.20 in order to apply it to results of Liu, Zureick-Brown, and the author [34]. We discussed above that the moments of the class groups of random Γ-extensions $K/\mathbb{F}_q(t)$ were found in the paper [34] (as $q \to \infty$), but this paper found, more generally, the moments of $\operatorname{Gal}(K^\#/K)$, where $K^\#$ is the maximal unramified extension of K that is prime to $|\Gamma|$, prime to $q(q-1)$, and split completely at infinity [34, THEOREM 1.4]. Moreover, the paper constructed a distribution on random groups with these moments [34, THEOREMS 1.2 AND 6.2]. Sawin applied his result [41, THEOREM 1.1] to conclude that (in a limit where $q \to \infty$ fast enough compared to n, similar to Theorem 2.16) the random profinite groups $\mathrm{Gal}(K^\#/K)$ converge in distribution to the group constructed in [34].

For quadratic extensions $K/\mathbb{F}_q(t)$, we can apply the work of Liu, Zureick-Brown, and the author [34], the homological stability result of Ellenberg, Venkatesh, and Westerland [19], and Sawin's result Theorem 2.20, and find the limiting distribution of the maximal unramified odd extension of K when $q, n \to \infty$ in any way. Let X be a random profinite group with an action of $\mathbb{Z}/2\mathbb{Z}$ with distribution μ_1 from [34, SECTION 4] (with $\Gamma = \mathbb{Z}/2\mathbb{Z}$). The measure of this distribution on basic opens is given explicitly in [34, EQUATION (4.14)]. Let $\mathcal{F}_m$ be the free odd profinite group on m generators, with a $\mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle$ action inverting each of the generators, and let y_i be independent random elements of $\mathcal{F}_m$ from Haar measure. Then in [34, SECTION 3], it is shown that $\mathcal{F}_m/\langle y_1^{-1}\sigma(y_1), \dots, y_{m+1}^{-1}\sigma(y_{m+1})\rangle$ converge in distribution to X, as $m \to \infty$. Let X_P be the pro-P completion (i.e., the inverse limit of all the finite P-group quotients) of X.

Theorem 2.23. *Let P be a finite set of odd primes. Let $K_{q,n}$ be a uniform random quadratic extension K of $\mathbb{F}_q(t)$, split completely over ∞, with* $\mathrm{Nm}\,\mathrm{Disc}\,K/\mathbb{F}_q(t) \le q^n$. *Let K^P be the maximal unramified extension of K, split completely at infinity, all of whose finite subextensions have degree a product of primes in P. Let $X_{q,n} = \mathrm{Gal}(K^P_{q,n}/K_{q,n})$.*

Then as $q, n \to \infty$ in any way such that q is odd, relatively prime to the primes in P, and $q - 1$ is relatively prime to the primes in P, then

$$X_{q,n} \text{ converge in distribution to } X_P.$$

Proof. Let $\Gamma = \mathbb{Z}/2\mathbb{Z}$. We follow [34, PROOF OF THEOREM 1.4], but will use the homological stability result of Ellenberg, Venkatesh, and Westerland [19]. Let H be a finite P-group with an action of Γ, such that the coinvariants H_Γ are trivial (note this is equivalent to the admissibility condition in [34], given the condition on P).

Let q be a prime power relatively prime to 2 and all the primes in P, and let $q - 1$ be relatively prime to all the primes in P. Let $E_\Gamma(n, q)$ be the set of quadratic extensions $K/\mathbb{F}_q(t)$, split completely at infinity, with $\mathrm{Nm}\,\mathrm{Disc}\,K/\mathbb{F}_q(t) = q^n$. Note n must be even for there to exist such a K (e.g., by the Riemann–Hurwitz formula). Let $G = H \rtimes \Gamma$. Let c be the set of elements of G of order 2, and note by the Schur–Zassenhaus Theorem this is a single conjugacy class of G. Then there are Hurwtiz schemes $\mathsf{Hur}^n_{G,c}$, $\mathsf{Hur}^n_{\Gamma,\Gamma\setminus\{1\}}$ constructed in [34], such that by [34, LEMMA 10.2]

$$[H : H^\Gamma] \sum_{K \in E_\Gamma(n,q)} \#\mathrm{Sur}_\Gamma\big(\mathrm{Gal}(K^P/K), H\big) = \#\mathsf{Hur}^n_{G,c}(\mathbb{F}_q)$$

and

$$\#E_\Gamma(n,q) = \#\mathsf{Hur}^n_{\Gamma,\Gamma\setminus\{1\}}(\mathbb{F}_q).$$

For n sufficiently large given G, by [34, THEOREM 10.4], we have that $\#\mathsf{Hur}^n_{G,c}$ and $\#\mathsf{Hur}^n_{\Gamma,\Gamma\setminus\{1\}}$ have the same number, z_n, of Frobenius fixed components over $\bar{\mathbb{F}}_q$. Moreover, z_n is positive for even n because we know $\mathbb{F}_q(t)$ has quadratic extensions split completely at infinity and so $\#\mathrm{Hur}^n_{\Gamma,\Gamma\setminus\{1\}}$ has $\mathbb{F}_q$-points. By the Grothendieck–Lefschetz trace formula, we have

$$\left|\#\mathrm{Hur}^n_{G,c}(\mathbb{F}_q) - z_n q^n\right| \le \sum_{j=0}^{2n-1} q^{j/2} \dim H^j_{c,ét}\big((\mathrm{Hur}^n_{G,c})_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell\big),$$

for some ℓ ([34, LEMMA 10.3] tells us $(\mathrm{Hur}^n_{G,c})_{\bar{\mathbb{F}}_q}$ is smooth and n-dimensional). By [34, LEMMA 10.3], we then have

$$\left|\#\mathrm{Hur}^n_{G,c}(\mathbb{F}_q) - z_n q^n\right| \le \sum_{j=0}^{2n-1} q^{j/2} \dim H^{2n-j}\big((\mathrm{Hur}^n_{G,c})_{\mathbb{C}}, \mathbb{Q}\big).$$

By [19, THEOREM 6.1, PROPOSITION 2.5] (their $\mathrm{CHur}^c_{G,n}$ is the topological space of the analytic topology of our $(\mathrm{Hur}^n_{G,c})_{\mathbb{C}}$ by [34, SECTION 11.3], and we can easily check their nonsplitting condition is satisfied here), there exist constants C and D, depending on G, such that $\dim H^k((\mathrm{Hur}^n_{G,c})_{\mathbb{C}}, \mathbb{Q}) \le CD^k$. Thus we have

$$\left|\#\mathrm{Hur}^n_{G,c}(\mathbb{F}_q) - z_n q^n\right| \le \sum_{j=0}^{2n-1} q^{j/2} C D^{2n-j}.$$

For $q \ge D^4$, we have

$$\left|\#\mathrm{Hur}^n_{G,c}(\mathbb{F}_q) - z_n q^n\right| \le \sum_{j=0}^{2n-1} C q^{n/2+j/4} \le \frac{2Cq^{n-1/4}}{1-q^{-1/4}}.$$

By the same argument, we have the same inequalities for $\mathrm{Hur}^n_{\Gamma,\Gamma\setminus\{1\}}$ Summing over even $n \le N$, we conclude that if $q, n \to \infty$ in any way, we have

$$\frac{1}{\#E_\Gamma(n,q)} \sum_{K \in E_\Gamma(n,q)} \#\,\mathrm{Sur}_\Gamma\big(\mathrm{Gal}(K^P/K), H\big) \to \left[H : H^\Gamma\right]^{-1}.$$

By [34, THEOREM 6.2], we see these are exactly the moments of the random Γ-group X_P described above. Thus applying Theorem 2.20, we conclude the result. ■

The methods of the paper [34] can find the moments of the maximal unramified extension of a random Γ extension $K/\mathbb{F}_q(t)$ even when we allow parts not prime to $q-1$, but the obstruction to proceeding is that there is no candidate conjectural random group with those moments. This brings us to the first case in this story when there was not an already known conjectural distribution that one was trying to show some distributions from number theory converged to. So we naturally turn to the existence and construction aspects of the moment problem.

All of the questions on moment problems for random groups discussed above have been reducible to questions of a countable list of linear equations in a countable number of variables, and whether they have a unique solution. The equations and variables are parametrized by groups, and the coefficients are given by group theoretic quantities (numbers of surjective homomorphisms). In Theorem 2.10, we made these equations quite explicit, and inverted the implicit infinite matrices by truncating them to finite matrices that we could explicitly invert. This is an approach that works well when the groups involved are $\mathbb{F}_p$-vector spaces, but it becomes less and less tractable as the groups get more complicated. For finite abelian groups, one relies on the classification of the groups and the ability to write a formula for the number of surjections from one to another. For nonabelian groups, there is no reasonable formulaic parametrization of the groups and their numbers of surjections. Theorem 2.20 is proved by a localization process that reduces the question to one only involving a smaller list of groups that can be classified and for which the number of surjections can be simply expressed.

All of these proofs of uniqueness, at least in principle, give some expression for the (only possible) solutions to these systems of equations. What then remains of the existence question? (1) The solutions must be nonnegative in order to describe a measure. (2) The determined values must further be shown to satisfy the equations. (3) In some cases, the solutions must be compatible in order to describe a measure.

We elaborate a bit on what these remaining problems are like. First we consider (1). In Theorem 2.10, we find an expression for x_0, the probability of the trivial group, as

$$\lim_{N\to\infty}\sum_{j=1}^{N}(V^{-1})_{1,j}M_{j-2},$$

where the M_j are the given moments, and the coefficients of the inverse matrix are given explicitly in (2.11). The other x_i are given similarly, with modified values of M_j. It is not clear whether one should expect a simple criterion for whether these values are nonnegative, but it seems conceivable that for a particular nice family of M_j of interest that one could, with work, prove the values of the x_i that are determined are indeed positive. Addressing (2), one could hope to prove for sufficiently bounded moments that these determined values satisfied the equations. We cannot see problem (3) above when the random groups are just $\mathbb{F}_p$-vector spaces, but even in the case of finite abelian p-groups, some approaches prove that the distribution on groups mod p is determined, and then that the distribution on groups mod p^2 is determined, etc. One can see this feature explicitly in the statement of Theorem 2.20. So, in such cases, to prove existence, one would have to check that the determined values were compatible and could be pieced together into a probability distribution.

The *construction* problem, which we have described above as giving *useful* formulas for the distribution, now turns on what useful means. The formulas for the distributions that arise from the uniqueness proofs above are generally infinite sums. One might not expect to solve this for general moments, but perhaps only for specific moments that arise in particular problems. We propose as one test of usefulness—can one detect if the distribution assigns value 0 to any particular basic open set? Note that the distributions on finite abelian groups we have seen above in Theorems 2.3 and 2.4 and in (2.7) all have this property. The distributions on non-abelian groups we have discussed, including those of Boston, Bush, and Hajir, and Liu, Zureick-Brown, and the author also have this property (see [11, LEMMA 4.8], [34, THEOREM 4.12]). Other tests for usefulness may come from the features of the desired application, but we emphasize that there can be a significant gap between having a formula for a distribution as an infinite sum, and being able to use that formula in practice to answer questions about the distribution.

We mention briefly forthcoming work of Sawin and the author on the moment problem for profinite groups. This work will strengthen Theorem 2.20 so that larger growing moments M_H are allowed, up to the point where the statement is no longer true (e.g., because of the example (2.7)). We also prove a general existence result addressing the problems (2) and (3) mentioned above. Our first applications are to problems where moments are known but the distribution is not known. The first of these applications is mentioned above, and is for the distribution of class groups or their nonabelian analogs, or order not prime to roots of unity in the base field $\mathbb{F}_q(t)$. The second is to the distribution of the profinite completion of random 3-manifolds (from random Heegaard splittings), as introduced by Dunfield and Thurston [18]. In these applications, we also solve the construction problem, e.g., we can describe explicitly the support of the limiting distribution, and we can use our formulas for the limiting distribution to answer open questions about the distributions from number theory and topology. Moreover, the 3-manifold application requires addressing situations where uniqueness does not actually hold, and we recover uniqueness with additional parity hypotheses, such as in Theorems 2.9, 2.10, and 2.14 above.

3. UNIVERSALITY

A central concept in probability theory is that of *universality*, which describes the ubiquitous phenomena that many input independent distributions can be combined to make an output distribution, and as the number of input distributions goes to infinity, the output distribution becomes quite insensitive to the input distributions. The first and most well-known example is the Central Limit Theorem.

Theorem 3.1 (Central Limit Theorem). *Let $X_1, X_2, \dots$ be independent, identically distributed random real numbers with finite mean $\mu = \mathbb{E}(X_i)$ and finite variance σ^2. Then as $n \to \infty$,*

$$\sqrt{n}\left(\frac{X_1 + \cdots + X_n}{n} - \mu\right)$$

converge in distribution to the normal distribution with mean 0 *and variance σ^2.*

Here the X_i are the input distributions, and their normalized sum is the output distribution, and we see that the output, asymptotically, only depends on the variance of the input distributions. The Central Limit Theorem is the tip of the iceberg, and probability theory is filled with further examples of this kind of phenomenon.

Here we discuss a somewhat newer line of inquiry, namely universality for random groups. In this case, the output distribution should be a random group, and the random group is somehow built out of the input distributions. One natural way to obtain such a random group is to start with a fixed random group F and take the quotient by random elements of F that we call relators. If F is a free abelian group, $F = \mathbb{Z}^n$, and we collect m random relators as the columns of a matrix M, then the quotient of F by our relators is the cokernel cok M (by definition of the cokernel). This shows that questions about random abelian groups built in this way can be rephrased as questions about cokernels of random integral matrices.

3.1. Random finite abelian groups

The simplest sort of groups to consider, as in our discussion above on the moment problem, are $\mathbb{F}_p$-vector spaces. Let $F = \mathbb{F}_p^n$. If M is an $n \times m$ matrix with coefficients in $\mathbb{F}_p$, then the quotient of F by the columns of M, i.e., $\operatorname{cok} M$, has rank equal to $n - \operatorname{rank} M = \operatorname{corank} M$. Hence we translate questions about random $\mathbb{F}_p$-vector spaces into questions about ranks of random matrices over $\mathbb{F}_p$. We note here that determining the rank distribution of random matrices over $\mathbb{F}_p$ is a simple exercise if the matrices are uniformly distributed. The entire interest here is when the matrix coefficients (still independent) are drawn from a wide range of distributions, and in particular if there is a resulting universality in the distribution of the ranks. There is a long history of work on this question. Kozlov [30] showed a universality result for the ranks over $\mathbb{F}_2$, and Kovalenko and Levitskaja [29] showed a version over $\mathbb{F}_p$. Both works require that the matrix entries take all possible values with positive probability. Charlap, Rees, and Robbins [12] only determined the probability that a square matrix is invertible, but allowed more general matrix entries. Balakin [2], Blömer, Karp, and Welzl [8], and Cooper [17] determined the ranks for sparser matrices, with entries uniformly distributed over nonzero values. The most general result we know is the following result of Nguyen and the author.

Theorem 3.2 (Corollary of [38, THEOREM 4.1]). *Let p be a prime. Let u be a nonnegative integer and α_n a function of integers n such that for any constant $\Delta > 0$, for n sufficiently large we have $\alpha_n \geq \Delta(\log n)/n$. For every positive integer n, let M_n be a random $n \times (n+u)$ matrix with independent entries $\xi_{i,j,n} \in \mathbb{F}_p$ that satisfy*

$$\max_{a \in \mathbb{F}_p} \operatorname{Prob}(\xi_{i,j,n} = a) \leq 1 - \alpha_n$$

for every i, j, n. Then for every $r \geq 0$,

$$\lim_{n\to\infty} \operatorname{Prob}(\operatorname{cok} M_n \simeq \mathbb{F}_p^r) = \lim_{n\to\infty} \operatorname{Prob}(\operatorname{rank} M_n = n - r) = p^{-r(r+u)} \frac{\prod_{j=r+u+1}^{\infty}(1 - p^{-j})}{\prod_{j=1}^{r}(1 - p^{-j})}.$$

We see that there are separate universality classes for different u, i.e., different numbers of relations compared to the number of generators, but for fixed u a wide range of entry distributions all give random groups in the same universality class. Note that Theorem 3.2 does not require the matrix entries to be identically distributed. It also allows the matrices to be quite sparse. If $\operatorname{Prob}(\xi_{i,j,n} = 0) = 1 - (\log n)/n$, the matrix would have a row of all zeroes with (asymptotically) positive probability, and this crosses a threshold for the behavior of the random matrix, similar to the well-known threshold for the behavior of random graphs and sparse random matrices in other contexts.

Open Problem 3.3. Lower the bound on α_n in Theorem 3.2, as close to the $(\log n)/n$ threshold as possible (and similarly for Theorems 3.4 and 3.6 below).

We next consider finite abelian p-groups, and now $F = \mathbb{Z}_p^n$ (and $\mathbb{Z}_p$ are the p-adic integers). If we form a random group by taking $n + u$ random relators, then the group is $\operatorname{cok} M$, where M is the matrix whose columns are the relations. Indeed, Theorem 3.2 is actually a corollary of the following.

Theorem 3.4 ([38, THEOREM 4.1]). *Let p be a prime. Let u be a nonnegative integer and α_n a function of integers n such that for any constant $\Delta > 0$, for n sufficiently large we have $\alpha_n \geq \Delta(\log n)/n$. For every positive integer n, let M_n be a $n \times (n+u)$ matrix with independent entries $\xi_{i,j,n} \in \mathbb{Z}_p$ that satisfy*

$$\max_{a \in \mathbb{F}_p} \operatorname{Prob}\bigl(\xi_{i,j,n} \equiv a \pmod{p}\bigr) \leq 1 - \alpha_n$$

for every i, j, n. Then for every abelian p-group A, we have

$$\lim_{n \to \infty} \mathbb{P}\bigl(\operatorname{cok}(M_n) \simeq A\bigr) = \frac{1}{|A|^u |\operatorname{Aut}(A)|} \prod_{k=1}^{\infty} (1 - p^{-k-u}).$$

The proof of Theorem 3.4 builds heavily on the method in [47], but extends the statement to include the sparse regime.

Proof of Theorem 3.2. The probabilities in Theorem 3.4 sum over A to 1 to give a probability distribution for each u [47, LEMMA 3.2]. Thus it follows from Fatou's Lemma that we can simply add up the probabilities from Theorem 3.4 for groups of rank r to obtain the limiting probabilities in Theorem 3.2. This is done in [15, COROLLARY 6.5]. ■

When $u = 0$, the distribution in Theorem 3.4 is the Cohen–Lenstra distribution of X_{CL} we have mentioned above, and when $u = 1$ it is the distribution conjectured by Cohen and Lenstra [15] for the Sylow p-subgroups of class groups of real random quadratic fields (for p odd). Let us now put these class groups in the context of random matrices, following Venkatesh and Ellenberg [42, SECTION 4.1]. Let $K = \mathbb{Q}(\sqrt{D})$ for some negative (resp. positive) square-free integer D, and S be any finite set of primes of K that generate $\mathrm{Cl}(K)$. We write $\mathcal{O}_S^*$ for the S-units in the integers $\mathcal{O}_K$, and I_K^S for the abelian group of fractional ideals generated by the elements of S. Then

$$\mathrm{Cl}(K) = \operatorname{cok}(\mathcal{O}_S^* \to I_K^S), \tag{3.5}$$

where the map takes α to the ideal (α). So the Sylow p-subgroup of $\mathrm{Cl}(K)$ is $\operatorname{cok}(\mathcal{O}_S^* \otimes_{\mathbb{Z}} \mathbb{Z}_p \to I_K^S \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. Since I_K^S and $\mathcal{O}_S^*$ are both abelian groups of rank $|S|$ (resp. of ranks $|S|$ and $|S|+1$), we have written the Sylow p-subgroup of $\mathrm{Cl}(K)$ as a cokernel of a p-adic $n \times n$ matrix R_D (resp. $n \times (n+1)$ matrix). One can now view the Cohen–Lenstra conjecture for class groups of quadratic fields as asking whether universality of Theorem 3.4 extends to the random matrix R_D for random D. This point of view was a motivation for the paper [47].

Now we consider random finite abelian groups more generally. For a finite set P of primes, considering finite abelian P-groups turns out to be only notationally more challenging than considering abelian p-groups, and indeed [38, THEOREM 4.1] is proven in this slightly more general context. However, considering all primes at once is quite a bit more of a challenge, because there will always be primes large compared to n. Nguyen and the author develop a method to handle large primes (compared to n) and we prove the following.

Theorem 3.6 ([38, THEOREM 1.1]). *For integers $n, u \geq 0$, let $M_{n\times(n+u)}$ be an integral $n \times (n+u)$ matrix with entries i.i.d. copies of a random integer ξ_n, with*

$$\limsup_{p \text{ prime}} \max_{a\in\mathbb{F}_p} \operatorname{Prob}\bigl(\xi_n \equiv a \pmod{p}\bigr) \leq 1 - n^{-1+\epsilon}$$

and $|\xi_n| \leq n^T$ for any fixed parameters $0 < \epsilon < 1$ and $T > 0$ not depending on n. For any fixed finite abelian group A and $u \geq 0$,

$$\lim_{n\to\infty} \mathbb{P}\bigl(\operatorname{cok}(M_{n\times(n+u)}) \simeq A\bigr) = \frac{1}{|A|^u |\operatorname{Aut}(A)|} \prod_{k=u+1}^{\infty} \zeta(k)^{-1}, \tag{3.7}$$

where $\zeta(s)$ is the Riemann zeta function.

Note this theorem has nice corollaries like the probability that a random map as in Theorem 3.6 (for $u = 1$) from $\mathbb{Z}^{n+1} \to \mathbb{Z}^n$ is surjective is $\prod_{k=2}^{\infty} \zeta(k)^{-1} \approx 0.4358$. As in the proof of Theorem 3.2, one can obtain other probabilities as corollaries, such as (for $u \geq 1$) the probability that $\operatorname{cok}(M_{n\times(n+u)})$ is cyclic. However, when $u = 0$, the probabilities in Theorem 3.6 are all 0 (from the $\zeta(1)^{-1}$ term), so this theorem tells us little about the distribution of random abelian groups from n generators and n random relations. In [38, THEOREM 1.2] we do find the probability that $\operatorname{cok}(M_{n\times n})$ is cyclic, and in [38, THEOREM 2.4] more generally give the probability that $\operatorname{cok}(M_{n\times n})$ is any set of groups $\{A \times C | C \text{ cyclic}, p \nmid |C| \text{ for } 1 < p < Y\}$. However, we are not able to distinguish a factor of $\mathbb{Z}/p\mathbb{Z}$ for large p from one of $\mathbb{Z}/p^2\mathbb{Z}$, for example.

Open Problem 3.8. Find

$$\lim_{n\to\infty} \operatorname{Prob}\bigl(|\operatorname{cok} M_{n\times n}| \text{ is square-free}\bigr) = \lim_{n\to\infty} \operatorname{Prob}\bigl(|\det M_{n\times n}| \text{ is square-free}\bigr).$$

Note that finding the probability that a polynomial takes square-free values on even the nicest distributions of integers is difficult and generally open, but there has been some progress for certain discriminant polynomials by Bhargava [4] and Bhargava, Shankar, and Wang [6]

Open Problem 3.9. Extend Theorem 3.6 to nonidentical entries.

The first connection of the Cohen–Lenstra heuristics to random matrices came from work of Friedman and Washinton [23]. They considered the analog of the Cohen–Lenstra conjectures for quadratic extensions of $\mathbb{F}_q(t)$. In this case one can also describe the Sylow p-subgroup of the class group of K (or more precisely of the Pic^0) as the cokernel of a certain random $2g \times 2g$ random matrix $I - F$ over $\mathbb{Z}_p$, where I is the identity matrix, and F describes the action of Frobenius on the p-adic Tate module of the curve corresponding to K [23, PROPOSITION 2]. (Here p is *not* the characteristic of $\mathbb{F}_q$.) Friedman and Washington showed that the cokernels of random matrices from the (additive) Haar measure on $n \times n$ matrices over $\mathbb{Z}_p$, as $n \to \infty$, approach the Cohen–Lenstra distribution. However, the matrix F above is not just any matrix; since it acts on the Weil pairing by scaling the pairing by q, it lies in a generalized symplectic coset $\operatorname{GSp}_{2g}^q(\mathbb{Z}_p)$ ($\operatorname{GSp}_{2g}^q(\mathbb{Z}_p)$ is the coset of matrices M such that $M^t JM = qJ$, where J is an invertible alternating matrix, and in particular the $M \in \mathrm{GSp}^q_{2g}(\mathbb{Z}_p)$ are invertible). Friedman and Washington prove that the cokernels of random matrices $I - M$, where M is random from the (multiplicative) Haar measure on $\mathrm{GL}_{2g}(\mathbb{Z}_p)$, as $g \to \infty$, approach the Cohen–Lenstra distribution [23, SECTION 4]. Eventually, it was understood that this also holds for $I - M$, where M is random from the Haar induced measure on $\mathrm{GSp}^q_{2g}(\mathbb{Z}_p)$ and $\gcd(q-1, p) = 1$. (This is not clearly stated in the literature, but follows from work of Achter [1] and Ellenberg and Venkatesh [19] in a very round about way, as outlined by Garton [24, P.153].)

We can view these results as additional examples of random matrices in the universality class of Theorem 3.4, even though the matrices do not have independent entries, and also come from very special distributions. Another example that would fit into this category is Mészáros's theorem [37, THEOREM 1] that says that the Laplacians of uniform random d-regular directed graphs, for any $d \geq 3$, also have these limiting cokernel distributions. It is a very interesting problem to extend this universality to matrices with dependent entries but for broader classes of random matrices, where the degrees of freedom in choosing the distribution of random matrices is large. As an example, in [38, THEOREM 1.6], we extend universality to Laplacians of random matrices with independent entries (so matrices whose off-diagonal entries are independent and whose columns sum to 0), which includes Laplacians of directed Erdős–Rényi random graphs. However, this is a very special kind of dependency among entries for which the methods are well-suited.

Open Problem 3.10. Extend Theorem 3.4 to more classes of matrices with dependent entries.

Open Problem 3.11. Give a unified proof that multiple special classes of random matrices are in the universality class of Theorem 3.4.

3.2. Random finite abelian groups with additional structure

Of course, if the entries of the random matrices have too much dependence in some particular way, their cokernels may land in another universality class. For example, for symmetric matrices the author has proved the following.

Theorem 3.12 ([44]). *Let p be a prime and $0 < \alpha < 1$. For every positive integer n, let M_n be a symmetric random $n \times n$ matrix with independent entries $\xi_{i,j,n} \in \mathbb{Z}_p$ for $i \geq j$ that satisfy*

$$\max_{a \in \mathbb{F}_p} \mathrm{Prob}\big(\xi_{i,j,n} \equiv a \pmod{p}\big) \leq 1 - \alpha$$

for every i, j, n. Then for every abelian P-group A, we have

$$\lim_{n\to\infty} \mathbb{P}\big(\mathrm{cok}(M_n)_P \simeq A\big) = \frac{\#\{\textit{symmetric, bilinear, perfect } \phi : A \times A \to \mathbb{C}^*\}}{|A||\mathrm{Aut}(A)|} \prod_{k=0}^{\infty} \big(1 - p^{-2k-1}\big).$$

(Note the number of pairings can be described explicitly in terms of the partition corresponding to the group A [44, EQUATION (2)].)

Proof. Theorem 6.1 in [44] gives the moments, and then Theorem 2.5 shows they determine a unique distribution, and [13, THEOREM 2] gives formulas for the distribution when M_n is taken from Haar measure, as in [44, COROLLARY 9.2]. ∎

Nguyen and the author have forthcoming work in which we extend Theorem 3.12 to integer matrices (and all primes), analogous our results on $n \times n$ matrices over $\mathbb{Z}$ described above (including obtaining the probability that the cokernel is cyclic).

One way of understanding why some random groups are in a different universality class is that the groups may be naturally coming with further structure than just group structure. For example, the cokernel of a symmetric matrix over the integers (or $\mathbb{Z}_p$) [13, SECTION 1.1] comes with a natural symmetric bilinear pairing. Clancy, Leake, and Payne [14] suggested that for random graphs, the cokernels of the graph Laplacian, along with their symmetric pairing, should be distributed proportionally to $|A|^{-1}|\mathrm{Aut}(A, \langle\cdot,\cdot\rangle)|^{-1}$. If we sum these expressions over isomorphism classes of pairings for a fixed group, we exactly obtain the probabilities for groups in Theorem 3.12 (see [44, COROLLARY 9.2]). This reflects an important part of the philosophy of the Cohen–Lenstra–Martinet heuristics—that the natural distributions on algebraic objects must take into account all of the structure of the objects. For example, when considering class groups of Galois number fields with Galois group G, we consider the class group not just as a group but rather as a G-module, and the predicted probabilities for a particular G-module involve the number of automorphisms of the G-module (as a G-module). Since the distributions that arise from universality theorems are certainly natural, we would expect them to share this sensitivity to extra structure, and thus it makes sense that cokernels of symmetric matrices, since as such they have natural symmetric pairings, should be distributed in a distribution that sees those pairings.

Open Problem 3.13. Prove that the cokernels of random symmetric matrices as in Theorem 3.12, along with their pairings, are distributed as suggested by Clancy, Leake, and Payne [14, SECTION 4]. One might naturally use moments of groups with pairings, and the corresponding moment problem, as in [32, SECTION 8].

There are a few other classes of random groups that we know in this universality class. The result [44, THEOREM 1.1] extends Theorem 3.12 to cokernels of Erdős–Rényi random graph Laplacians, also known as sandpile groups or Jacobians of the graphs. Mészáros [37, THEOREM 1.2] extends Theorem 3.12 to sandpile groups of d-regular graphs for $d \geq 3$ (unless d is even and $p = 2$, in which case a different distribution arises, likely reflecting further structure of the pairing). Dunfield and Thurston [18, SECTION 8.7] show that the homology $H_1(M, \mathbb{F}_p)$ for a 3-manifold from a random Heegaard splitting of genus g as $g \to \infty$ approaches the universal distribution of Theorem 3.12, or more precisely the pushforward of that distribution to elementary abelian p-groups under the map $A \mapsto A/pA$. (See [44, COROLLARY 9.4] to see that this is indeed the pushforward.) Forthcoming work of Sawin and the author finds the distribution more generally of $H_1(M, \mathbb{Z}_p)$, along with the torsion linking pairing, of these random 3-manifolds, and finds that it is in the natural distribution suggested by Clancy, Leake, and Payne [14, SECTION 4]. So the presence of the symmetric pairing from the torsion linking pairing explains why the homology of random 3-manifolds appears in this universality class.

Open Problem 3.14. Prove that the sandpile groups of Erdős–Rényi random graphs (or uniform random d-regular graphs) along with their pairings, are distributed as suggested by Clancy, Leake, and Payne [14, SECTION 4].

There are, however, many more algebraic structures that are important in arithmetic statistics and other fields whose universality classes should be studied, such as random abelian groups with an action of a group, or random modules.

Open Problem 3.15. Prove an analog of Theorem 3.4 for $\mathbb{Z}_p[G]$-modules for a finite group G (with $p \nmid |G|$). More generally (as would be related to the Cohen–Lenstra–Martinet heuristics for non-Galois fields, see [43, SECTIONS 7–8]), prove an analog of Theorem 3.4 for random $\mathfrak{o}$-modules, where $\mathfrak{o}$ is a maximal order (over $\mathbb{Z}_p$) in a semisimple $\mathbb{Q}_p$-algebra.

Note that the reduction of Problem 3.15 mod p is a question about matrices over finite fields. So part of solving the above will include generalizing Theorem 3.2 from $\mathbb{F}_p$ to general finite fields $\mathbb{F}_q$. In this more general case, the requirement that the $\xi_{i,j,n}$ are not concentrated at a single point is not sufficient, and must be replaced with something like $\xi_{i,j,n}$ not concentrated on a translate of a subfield. Kahn and Komlós [27] have shown universality of the singularity probability of a random $n \times n$ matrix over $\mathbb{F}_q$ under such a condition.

Open Problem 3.16. For $\mathfrak{o}$ a maximal order (over $\mathbb{Z}_p$) in a semisimple $\mathbb{Q}_p$-algebra, with an order two automorphism σ, such as $\mathfrak{o}$ being the ring of integers of the unramified quadratic extension of $\mathbb{Q}_p$, or $\mathfrak{o} = \mathbb{Z}_p \times \mathbb{Z}_p$, prove an analog of Theorem 3.12 for random σ-Hermitian matrices (i.e. M such that $\sigma(M) = M^t$).

3.3. Random nonabelian groups

We now turn to universality questions for nonabelian random groups, which are largely unstudied, but we expect contain much potential. One naturally starts with a free group (or free profinite group) F_n and takes the quotient by independent random relations in some way that involves many independent choices for each relations. As $n \to \infty$, one hopes that the limiting distribution is somewhat insensitive to the distribution from which the relations are chosen. The first stumbling block when considering such questions is that it is less clear how to take a random relation built up from many independent choices. When the relation was in $\mathbb{F}_p^n$ or $\mathbb{Z}_p^n$, we could just take each coordinate independently. However, if F_n is the free group (or free profinite group) on n generators, there are not analogous coordinates in F_n. In the case of random nilpotent groups, one might consider using Mal'cev coordinates. Another way to characterize the probability measures on $\mathbb{Z}_p^n$ from which we drew relations above, e.g., in Theorem 3.4, is that they are not concentrated at a point in any finite simple quotient, so it may be interesting to consider the nonabelian version of that condition. While it is not so clear what the parameters for the universality class should be, one has a natural target for the universal distribution from a result of Liu and the author on the quotient of the free group by random relations. Let $\mathcal{G}$ be the set of isomorphism classes of profinite groups with finitely many surjections to any finite group. (This is $\mathcal{G}$ from Section 2.4 with $\Gamma = 1$, and we consider the same topology on it as defined there.)

Theorem 3.17 ([33, THEOREM 1.1]). *For every integer u, there is a random group X_u in $\mathcal{G}$ whose measure is described explicitly on each basic open* [33, EQUATION (3.2)]. *If F_n is the free profinite group on n generators, and r_i are independent random elements of F_n drawn from Haar measure, then as $n \to \infty$ the quotients*

$$F_n/\langle r_1, \dots, r_{n+u}\rangle \quad \textit{weakly converge in distribution to } X_u.$$

As in [33, SECTION 14], one can consider usual (not profinite) free group F_n and take random relations obtained from a random walk on F_n. However, as the length of the random walk goes to infinity, these relation become equidistributed with respect to Haar measure, and so this is not really a new example for the universality class.

Open Problem 3.18. Find some more general hypotheses for a distribution on F_n from which one can draw independent relations so that Theorem 3.17 still holds.

While it would be nice to have hypotheses that allow a wide range of distributions, i.e., a universality theorem, it would even be interesting to find other specific random groups converging to the distributions X_u. We give one example here, which is a nonabelian analog of the result of Friedman and Washington on cokernels of $I - M$, where M is random from the Haar measure on $\mathrm{GL}_n(\mathbb{Z}_p)$.

Theorem 3.19. *Let F_n be the free profinite group on n generators, and let* $\mathrm{Aut}(F_n)$ *be the group of (continuous) automorphisms of F_n, which is a profinite group* [40, COROLLARY 4.4.4]. *Let $I \in$* $\mathrm{Aut}(F_n)$ *be the identity and let α_n be a random element of* $\mathrm{Aut}(F_n)$ *with respect to Haar measure. Then, as $n \to \infty$,*

$$F_n/\bigl\langle \alpha_n(x)x^{-1} \mid x \in F_n\bigr\rangle \quad \textit{weakly converge in distribution to } X_0,$$

(where X_0 is defined as in Theorem 3.17).

We will compute the moments of these random groups, and then apply Corollary 2.22 from Sawin's result on the moment problem. To do that, we first need the moments of X_0. While it is an easy to see that for independent Haar relations r_i, we have

$$\lim_{n\to\infty} \mathbb{E}\bigl(\#\,\mathrm{Sur}\bigl(F_n/\langle r_1, \dots, r_{n+u}\rangle, A\bigr)\bigr) = 1,$$

it does require some argument to interchange the limit in n and the expectation and obtain these same moments for X_0.

Lemma 3.20. *Let X_0 be defined as in Theorem 3.17. Then for any finite group H, we have*

$$\mathbb{E}\bigl(\mathrm{Sur}(X_0, H)\bigr) = 1.$$

Proof. We follow the strategy of [34, THEOREM 6.2] adapted to our situation. Let F_n be the free profinite group on n generators and let Z_n be the random profinite group $F_n/\langle r_1, \dots, r_n\rangle$, where the r_i are random elements of F_n from Haar measure. For any positive integer ℓ, let $\mathcal{C}_\ell$ be the set of finite groups of order at most ℓ. We consider the following function defined for any positive integer ℓ and any finite group G of level with $G^{\mathcal{C}_\ell} \simeq G$,

$$f_n(G,\ell) = \mathbb{E}\big(\big|\operatorname{Sur}(Z_n, H)\big| \times \mathbb{1}_{{Z_n}^{\mathcal{C}_\ell} \simeq G}\big),$$

where $\mathbb{1}_{{Z_n}^{\mathcal{C}_\ell} \simeq G}$ is the indicator function of ${Z_n}^{\mathcal{C}_\ell} \simeq G$. We let $\pi_{F_n} \colon F_n \to (F_n)^{\mathcal{C}_\ell}$ and $\pi_H : H \to H^{\mathcal{C}_\ell}$ be the natural quotient maps. Each $\phi \in \operatorname{Sur}(F_n, H)$ induces a map $\overline{\phi} \in \operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, H^{\mathcal{C}_\ell})$. By the definition of random group Z_n, we have

$$\begin{aligned} &\mathbb{E}\big(\big|\operatorname{Sur}(Z_n, H)\big| \times \mathbb{1}_{{Z_n}^{\mathcal{C}_\ell} \simeq G}\big) \\ &\quad = \sum_{\phi \in \operatorname{Sur}(F_n, H)} \operatorname{Prob}\big(r_1, \dots, r_n \in \ker \phi \text{ and } (F_n)^{\mathcal{C}_\ell} / \big\langle \pi_{F_n}(r_1), \dots, \pi_{F_n}(r_n)\big\rangle \simeq G\big). \end{aligned} \tag{3.21}$$

Given $\phi \in \operatorname{Sur}_\Gamma(F_n, H)$ and $y_1, \dots, y_n \in \ker \overline{\phi}$, we have that

$$\operatorname{Prob}\big(r_1, \dots, r_n \in \ker \phi \mid \pi_{F_n}(r_i) = y_i \text{ for all } i\big) = \frac{|H^{\mathcal{C}_\ell}|^n}{|H|^n}.$$

This follows from the straightforward calculation that

$$\big|\pi_{F_n}^{-1}(y_i) \cap \ker \phi\big| = |F_n|\big|H^{\mathcal{C}_\ell}\big| / \big(\big|F_n^{\mathcal{C}_\ell}\big||H|\big).$$

Then, summing over choices of $y_i \in \ker \overline{\phi}$ such that $(F_n)^{\mathcal{C}_\ell} / \langle y_1, \dots, y_n\rangle \simeq G$, we have

$$\begin{aligned} &\operatorname{Prob}\left(\begin{matrix} r_1, \dots, r_n \in \ker \phi \text{ and} \\ (F_n)^{\mathcal{C}_\ell} / \big\langle \pi_{F_n}(r_1), \dots, \pi_{F_n}(r_n)\big\rangle \simeq G \end{matrix} \;\middle|\; \begin{matrix} \pi_{F_n}(r_i) \in \ker \overline{\phi} \text{ for all } i \text{, and} \\ (F_n)^{\mathcal{C}_\ell} / \big\langle \pi_{F_n}(r_1), \dots, \pi_{F_n}(r_n)\big\rangle \simeq G \end{matrix}\right) \\ &\quad = \frac{|H^{\mathcal{C}_\ell}|^n}{|H|^n}. \end{aligned}$$

Thus (3.21) is equal to

$$\begin{aligned} &\frac{|H^{\mathcal{C}_\ell}|^n}{|H|^n} \sum_{\phi \in \operatorname{Sur}(F_n, H)} \operatorname{Prob}\left(\begin{matrix} \pi_{F_n}(r_i) \in \ker \overline{\phi} \text{ for all } i \text{, and} \\ (F_n)^{\mathcal{C}_\ell} / \big\langle \pi_{F_n}(r_1), \dots, \pi_{F_n}(r_n)\big\rangle \simeq G \end{matrix}\right) \\ &\quad = \frac{|H^{\mathcal{C}_\ell}|^n}{|H|^n} \sum_{\phi \in \operatorname{Sur}(F_n, H)} \frac{\#\left\{(\tau, \pi) \;\middle|\; \begin{matrix} \tau \in \operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, G) \\ \pi \in \operatorname{Sur}(G, H^{\mathcal{C}_\ell}) \\ \text{and } \pi \circ \tau = \overline{\phi} \end{matrix}\right\}}{|\operatorname{Aut}(G)||G|^n} P_{0,n}(U_{\mathcal{C}_\ell, G}), \end{aligned} \tag{3.22}$$

where $P_{0,n}(U_{\mathcal{C}_\ell, G})$ is defined in [33] just before Lemma 9.5, and is the probability that n independent uniform random elements in the kernel of $(F_n)^{\mathcal{C}_\ell} \to G$ generate that kernel as a normal subgroup (as worked out in the proof of [33, THEOREM 8.1]). (To explain the above equality a bit more: if $(F_n)^{\mathcal{C}_\ell} / \langle \pi_{F_n}(r_1), \dots, \pi_{F_n}(r_n)\rangle \simeq G$ then there is a choice of $\tau \in \operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, G)$ inducing that isomorphism, whose $\operatorname{Aut}(G)$ orbit is unique, and $\bar{\phi}$ must factor through τ since $\pi_{F_n}(r_i) \in \ker \overline{\phi}$. Given a τ, the probability that the relations are in $\ker \tau$ and generate it as a normal subgroup is $|G|^{-n} P_{0,n}(U_{\mathcal{C}_\ell, G})$.)

On the other hand, let $\overline{\phi} \in \operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, H^{\mathcal{C}_\ell})$. Then the composition map $\rho := \overline{\phi} \circ \pi_{F_n}$ is a surjection $F_n \to H^{\mathcal{C}_\ell}$. The number of $\phi \in \operatorname{Sur}(F_n, A)$ such that ϕ induces $\overline{\phi}$ we denote by $\operatorname{Sur}(\rho, \pi_H)$. It is easy to see that

$$\frac{|\operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, G)|}{|G|^n} \leq 1 \quad \text{and} \quad \lim_{n\to\infty} \frac{|\operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, G)|}{|G|^n} = 1,$$

and similarly

$$\frac{|\operatorname{Sur}(\rho, \pi_H)|}{|H|^n |H^{\mathcal{C}_\ell}|^{-n}} \leq 1, \quad \lim_{n\to\infty} \frac{|\operatorname{Sur}(\rho, \pi_H)|}{|H|^n |H^{\mathcal{C}_\ell}|^{-n}} = 1.$$

Then by (3.22), we obtain that $f_n(G,\ell) = g_n(G,\ell) P_{0,n}(U_{\mathcal{C}_\ell, G})$ where

$$g_n(G,\ell) = \frac{|H^{\mathcal{C}_\ell}|^n |\operatorname{Sur}(\rho, \pi_H)|| \operatorname{Sur}((F_n)^{\mathcal{C}_\ell}, G)||\operatorname{Sur}(G, H^{\mathcal{C}_\ell})|}{|H|^n |G|^n |\operatorname{Aut}(G)|} \quad \text{and}$$

$$g(G,\ell) := \lim_{n\to\infty} g_n(G,\ell) = \frac{|\operatorname{Sur}(G, H^{\mathcal{C}_\ell})|}{|\operatorname{Aut}(G)|}.$$

Now we apply **[34, LEMMA 5.10]**, where condition (1) holds by definition, (2) from the above, and (3) follows from the definition of $f_n(G,\ell)$. This allows us to conclude, for every ℓ,

$$\sum_{\substack{G \\ G^{\mathcal{C}_\ell} \simeq G}} \lim_{n\to\infty} f_n(G,\ell) = \lim_{n\to\infty} f_n(\text{trivial group}, 1) = \lim_{n\to\infty} \mathbb{E}\big(\big|\operatorname{Sur}(X_n, H)\big|\big) = 1. \quad (3.23)$$

When ℓ is sufficiently large such that $H^{\mathcal{C}_\ell} \simeq H$,

$$\lim_{n\to\infty} f_n(G,\ell) = \lim_{n\to\infty} \big|\operatorname{Sur}(G,H)\big| \operatorname{Prob}\big((Z_n)^{\mathcal{C}_\ell} \simeq G\big) = \big|\operatorname{Sur}(G,H)\big| \operatorname{Prob}\big((X_0)^{\mathcal{C}_\ell} \simeq G\big),$$

where the last equality is by Theorem 3.17. Hence (3.23) gives the desired result in the lemma. ■

Proof of Theorem 3.19. We compute the moments of $F_n / \langle \alpha_n(x) x^{-1} \mid x \in F_n \rangle$. Consider a fixed finite group H. If H can be generated by n elements, then there are some number of surjections $\phi : F_n \to H$. Those surjections that factor through the quotient

$$F_n / \big\langle \alpha_n(x) x^{-1} \mid x \in F_n \big\rangle$$

are exactly those ϕ such that $\phi\alpha = \phi$. So

$$\mathbb{E}\big(\#\operatorname{Sur}\big(F_n / \big\langle \alpha_n(x) x^{-1} \mid x \in F_n \big\rangle, H\big)\big) = \sum_{\phi \in \operatorname{Sur}(F_n, H)} \operatorname{Prob}(\phi\alpha = \alpha).$$

The action of $\operatorname{Aut}(F_n)$ on $\operatorname{Sur}(F_n, H)$ is transitive **[35, PROPOSITION 2.2]**, and factors through a finite group. So $\operatorname{Prob}(\phi\alpha = \alpha) = |\operatorname{Sur}(F_n, H)|^{-1}$. Thus, as long as H can be generated by n elements, we have

$$\mathbb{E}\big(\#\operatorname{Sur}\big(F_n / \big\langle \alpha_n(x) x^{-1} \mid x \in F_n \big\rangle, H\big)\big) = 1.$$

Thus we can use Theorem 2.20 and Lemma 3.20 to conclude the theorem. ■

Of course, if any kind of universality result can be proven for nonabelian random groups, it would then be interesting to extend the methods to particular nonabelian groups with additional structure that are arising in number theory and topology. So far the applications of these sort of universality methods for random groups have largely been in combinatorics. We expect that as the methods become developed, there will be further applications, including in number theory and topology.

ACKNOWLEDGMENTS

Much of this paper is based on the author's work with coauthors Nigel Boston, Hoi Nguyen, Yuan Liu, Will Sawin, Weitong Wang, and David Zureick-Brown, and we thank them for all the insights gained from these collaborations. The outlook in this paper also benefited from useful conversations with Jordan Ellenberg, Aaron Landesman, Sam Payne, Bjorn Poonen, and Philip Matchett Wood. The author would like to thank Yuan Liu, Hoi Nguyen, and Will Sawin for useful feedback on an earlier draft of this paper.

FUNDING

This work was done with the support of a Packard Fellowship for Science and Engineering, National Science Foundation Waterman Award DMS-2140043, and National Science Foundation grant DMS-2052036.

REFERENCES

[1] J. D. Achter, Results of Cohen–Lenstra type for quadratic function fields. In *Computational arithmetic geometry*, pp. 1–7, Contemp. Math. 463, Amer. Math. Soc., Providence, RI, 2008.

[2] G. V. Balakin, The distribution of the rank of random matrices over a finite field. *Akad. Nauk SSSR. Teor. Veroâtn. Primen.* **13** (1968), 631–641.

[3] A. Bartel and H. W. Lenstra, On class groups of random number fields. *Proc. Lond. Math. Soc.* **121** (2020), no. 4, 927–953.

[4] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials. 2014, arXiv:1402.0031.

[5] M. Bhargava, D. M. Kane, H. W. Jr. Lenstra, B. Poonen, and E. Rains, Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves. *Camb. J. Math.* **3** (2015), no. 3, 275–321.

[6] M. Bhargava, A. Shankar, and X. Wang, Squarefree values of polynomial discriminants I. 2016, arXiv:1611.09806.

[7] P. Billingsley, *Probability and measure. Second edn*. Wiley Ser. Prob. Math. Stat., Prob. Math. Stat., John Wiley & Sons, Inc., New York, 1986.

[8] J. Blömer, R. Karp, and E. Welzl, The rank of sparse random matrices over finite fields. *Random Structures Algorithms* **10** (1997), no. 4, 407–419.

[9] N. Boston, M. R. Bush, and F. Hajir, Heuristics for p-class towers of imaginary quadratic fields. *Math. Ann.* **368** (2017), no. 1–2, 633–669.

[10] N. Boston, M. R. Bush, and F. Hajir, Heuristics for p-class towers of real quadratic fields. *J. Inst. Math. Jussieu* **20** (2021), no. 4, 1429–1452.

[11] N. Boston and M. M. Wood, Non-abelian Cohen–Lenstra heuristics over function fields. *Compos. Math.* **153** (2017), no. 7, 1372–1390.

[12] L. S. Charlap, H. D. Rees, and D. P. Robbins, The asymptotic probability that a random biased matrix is invertible. *Discrete Math.* **82** (1990), no. 2, 153–163.

[13] 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.* (2015), 1–23.

[14] J. Clancy, T. Leake, and S. Payne, A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs. *Exp. Math.* **24** (2015), no. 1, 1–7.

[15] H. Cohen and H. W. Jr. Lenstra, Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, pp. 33–62, Lecture Notes in Math. 1068, Springer, Berlin, 1984.

[16] H. Cohen and J. Martinet, étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.* **404** (1990), 39–76.

[17] C. Cooper, On the distribution of rank of a random matrix over a finite field. *Random Structures Algorithms* **17** (2000), no. 3–4, 197–212.

[18] N. M. Dunfield and W. P. Thurston, Finite covers of random 3-manifolds. *Invent. Math.* **166** (2006), no. 3, 457–521.

[19] 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), no. 3, 729–786.

[20] T. Feng, A. Landesman, and E. Rains, The geometric distribution of Selmer groups of elliptic curves over function fields. 2020, arXiv:2003.07517.

[21] É. Fouvry and J. Klüners, Cohen–Lenstra heuristics of quadratic number fields. In *Algorithmic number theory*, edited by F. Hess, S. Pauli, and M. Pohst, pp. 40–55, Lecture Notes in Comput. Sci. 4076, Springer, Berlin–Heidelberg, 2006.

[22] É. Fouvry and J. Klüners, On the 4-rank of class groups of quadratic number fields. *Invent. Math.* **167** (2006), no. 3, 455–513.

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

[24] D. Garton, Random matrices, the Cohen–Lenstra heuristics, and roots of unity. *Algebra Number Theory* **9** (2015), no. 1, 149–171.

[25] F. Gerth III, Extension of conjectures of Cohen and Lenstra. *Expo. Math.* **5** (1987), no. 2, 181–184.

[26] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem. II. *Invent. Math.* **118** (1994), no. 2, 331–370.

[27] J. Kahn and J. Komlós, Singularity Probabilities for Random Matrices over Finite Fields. *Combin. Probab. Comput.* **10** (2001), no. 02, 137–157.

[28] J. Klys, The distribution of p-torsion in degree p cyclic fields. *Algebra Number Theory* **14** (2020), no. 4, 815–854.

[29] I. N. Kovalenko and A. A. Levitskaja, Limiting behavior of the number of solutions of a system of random linear equations over a finite field and a finite ring. *Dokl. Akad. Nauk SSSR* **221** (1975), no. 4, 778–781.

[30] M. V. Kozlov, On the rank of matrices with random Boolean elements. *Sov. Math., Dokl.* **7** (1966), 1048–1051.

[31] J. B. Lewis, R. I. Liu, A. H. Morales, G. Panova, S. V. Sam, and Y. X. Zhang, Matrices with restricted entries and q-analogues of permutations. *J. Comb.* **2** (2011), no. 3, 355–395.

[32] M. Lipnowski, W. Sawin, and J. Tsimerman, Cohen–Lenstra heuristics and bilinear pairings in the presence of roots of unity. 2020, arXiv:2007.12533.

[33] Y. Liu and M. M. Wood, The free group on n generators modulo $n + u$ random relations as n goes to infinity. *J. Reine Angew. Math.* **2020** (2020), no. 762, 123–166.

[34] Y. Liu, M. M. Wood, and D. Zureick-Brown, A predicted distribution for Galois groups of maximal unramified extensions. 2019, arXiv:1907.05002.

[35] A. Lubotzky, Pro-finite presentations. *J. Algebra* **242** (2001), no. 2, 672–690.

[36] G. Malle, Cohen–Lenstra heuristic and roots of unity. *J. Number Theory* **128** (2008), no. 10, 2823–2835.

[37] A. Mészáros, The distribution of sandpile groups of random regular graphs. *Trans. Amer. Math. Soc.* **373** (2020), no. 9, 6529–6594.

[38] H. H. Nguyen and M. M. Wood, Random integral matrices: universality of surjectivity and the cokernel. *Invent. Math.* (2021). DOI 10.1007/s00222-021-01082-w.

[39] B. Poonen and E. Rains, Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.* **25** (2012), no. 1, 245–269.

[40] L. Ribes and P. Zalesskii, *Profinite groups. Second edn., Ergebnisse Der Mathematik Und Ihrer Grenzgebiete. 3. Folge*. Ergeb. Math. Grenzgeb. (3) 40, Springer, Berlin, 2010.

[41] W. Sawin, Identifying measures on non-abelian groups and modules by their moments via reduction to a local problem. 2020, arXiv:2006.04934.

[42] A. Venkatesh and J. S. Ellenberg, Statistics of number fields and function fields. In *Proceedings of the International Congress of Mathematicians. Volume II*, pp. 383–402, Hindustan Book Agency, New Delhi, 2010.

[43] W. Wang and M. Wood, Moments and interpretations of the Cohen–Lenstra–Martinet heuristics. *Comment. Math. Helv.* **96** (2021), no. 2, 339–387.

[44] M. Wood, The distribution of sandpile groups of random graphs. *J. Amer. Math. Soc.* **30** (2017), no. 4, 915–958.

[45] M. M. Wood, On the probabilities of local behaviors in abelian field extensions. *Compos. Math.* **146** (2010), no. 1, 102–128.

[46] M. M. Wood, Cohen–Lenstra heuristics and local conditions. *Res. Number Theory* **4** (2018), no. 4, 41.

[47] M. M. Wood, Random integral matrices and the Cohen–Lenstra heuristics. *Amer. J. Math.* **141** (2019), no. 2, 383–398.

MELANIE MATCHETT WOOD

Department of Mathematics, Harvard University, Science Center Room 325,
1 Oxford Street, Cambridge, MA 02138, USA, mmwood@math.harvard.edu