THE FREE GROUP ON n GENERATORS MODULO $n + u$ RANDOM RELATIONS AS n GOES TO INFINITY

YUAN LIU AND MELANIE MATCHETT WOOD

ABSTRACT. We show that, as n goes to infinity, the free group on n generators, modulo $n+u$ random relations, converges to a random group that we give explicitly. This random group is a non-abelian version of the random abelian groups that feature in the Cohen-Lenstra heuristics. For each n, these random groups belong to the few relator model in the Gromov model of random groups.

1. INTRODUCTION

For an integer u and positive integers n, we study the random group given by the free group F_n on n generators modulo $n + u$ random relations. In particular we find that these random groups have a nice limiting behavior as $n \to \infty$ and we explicitly describe the limiting random group.

There are two ways to take relations in a "uniform" way: 1)complete F_n to the profinite free group $\hat{F}_n$ on n generators and take relations with respect for Haar measure, or 2)take relations from F_n uniformly among words up to length ℓ and then let $\ell \to \infty$. In Proposition 14.1, we show that the random groups obtained from the second method weakly converge, as $\ell \to \infty$, to the random groups obtained from the first method.

For a positive integer n, let $\hat{F}_n$ be the profinite free group on n generators. For an integer u, we define the random group $X_{u,n}$ by taking the quotient of $\hat{F}_n$ by (the closed, normal subgroup generated by) $n + u$ independent random generators, taken from Haar measure on $\hat{F}_n$. We need to define a topology to make precise the convergence of $X_{u,n}$ as $n \to \infty$.

Let S be a set of (isomorphism classes of) finite groups. Let $\bar{S}$ be the smallest set of groups containing S that is closed under taking quotients, subgroups, and finite direct products. For a profinite group G, we write $G^{\bar{S}}$ for its pro-$\bar{S}$ completion. We consider the set $\mathcal{P}$ of isomorphism classes of profinite groups G such that $G^{\bar{S}}$ is finite for all finite sets S of finite groups. All finitely generated profinite groups are in $\mathcal{P}$ and all groups in $\mathcal{P}$ are small in the sense of [FJ08, Section 16.10]. We define a topology on $\mathcal{P}$ in which the basic opens are, for each finite set S of finite groups and finite group H, the sets $U_{S,H} := \{G \mid G^{\bar{S}} \simeq H\}$.

Theorem 1.1. *Let u be an integer. Then there is a probability measure μ_u on $\mathcal{P}$ for the σ-algebra of Borel sets such that as $n \to \infty$, the distributions of $X_{u,n}$ weakly converge to μ_u.*

We give these μ_u explicitly in fact. See Equation (3.2) for a formula for μ_u on each basic open, and see Section 12 for several other interesting examples of the values of these measures. In fact, we prove in Theorem 11.4 a stronger form of convergence than weak convergence, which, in particular, tell us the measure of any finite group. In particular, we have

$$(1.2) \qquad \mu_u(\text{trivial group}) = \prod_{\substack{G \text{ finite simple} \\ \text{abelian group}}} \prod_{i=u+1}^{\infty} (1 - |G|^{-i}) \prod_{\substack{G \text{ finite simple} \\ \text{non-abelian group}}} e^{-|\operatorname{Aut}(G)|^{-1}|G|^{-u}},$$

which is $\approx .4357$ when $u = 1$. The abelian group version of this problem has been well-studied, as the limiting groups when $u = 0, 1$ are the random groups of the Cohen-Lenstra heuristics. The first factor above, as a product over primes, is very familiar from the random groups of the Cohen-Lenstra heuristics, but here it naturally appears as part of a product over all finite simple groups.

Cohen and Lenstra [CL84] defined certain random abelian groups that they predicted gave the distribution of class groups of random quadratic fields. Friedman and Washington [FW89] later realized that these random abelian groups arose as the limits of cokernels of random matrices, which is just a rewording of the abelianization of our construction above. These random abelian groups are universal, in the sense that, as $n \to \infty$, taking $\mathbb{Z}^n$ modulo almost any collection of $n + u$ independent relations will give these same random abelian groups, even if the relations are taken from strange and lopsided distributions [Woo15].

One motivation for our work is to develop a non-abelian version of the random abelian groups of Cohen and Lenstra, in order to eventually be able to model non-abelian versions of class groups of random number fields. Boston, Bush, and Hajir [BBH16] have defined random pro-p groups that they conjecture model the pro-p generalizations of class groups of random imaginary quadratic fields. In their definition, they were able to use special properties of p-groups to give a definition that avoids the limit as $n \to \infty$ that we study above (or rather, reduces the question of the limit as $n \to \infty$ to the abelian case, which was already understood).

There is a large body of work on the Gromov, or density, model of random groups (see [Oll05] for an excellent introduction). In this model, one takes F_n modulo $r(\ell)$ random relations uniform among words of length ℓ, and studies the behavior as $\ell \to \infty$. When $r(\ell)$ grows like $(2n - 1)^{d\ell}$ this is called the density d model. There has been a great amount of work to understand, as $\ell \to \infty$, what properties hold asymptotically almost surely for these groups (e.g see [Oll05, Oll10] for an overview and [CW15, KK13, Mac16, OW11] for some more recent examples). Our $X_{u,n}$ are limits as $\ell \to \infty$ of density 0 models of these random groups. In fact, slightly different density 0 models introduced by Gromov [Gro87] and Arzhantseva and Ol'shanskii [AO96] were predecessors to the work on the density model for arbitrary d and are also the subject of a large body of work. However, the emphasis of our work is different from much of the previous work on these models of random groups. That work has often emphasized a random group with given generators, and we consider only the isomorphism class of the group and focus on the convergence to a limiting random variable as the number of generators goes to infinity. Properties that hold asymptotically almost surely as $\ell \to \infty$ may not hold of the limiting random variable. For example, in our topology, any Gromov random group with $r(\ell) \to \infty$ weakly converges to the trivial group, yet at low enough density these groups are asymptotically almost surely not trivial (see Proposition 14.2 and Remark 14.3). Our topology is aimed at understanding finite quotients of groups, and is rather different than the topology due to Chabauty [Cha50] and Grigorchuk [Gri84] on the space of marked groups that emphasizes the geometry of the Cayley graphs but isn't well behaved on isomorphism classes of groups.

The previous work with the closest emphasis to ours is that of Dunfield and Thurston [DT06]. They studied F_n modulo r random relations (with both methods described above of taking relations) in order to contrast those random groups with random 3-manifold groups. Their main consideration was the probability that these random groups (for fixed n and r)

had a quotient map to a fixed finite group. They do observe [DT06, Theorem 3.10] that for a fixed non-abelian finite simple group G, the distribution of the number of quotient maps to G has a Poisson limiting behavior as $n \to \infty$; this is the first glimpse of the nice limiting behavior as $n \to \infty$ that we study in this paper.

Jarden and Lubotzky [JL06] studied the normal subgroup of $\hat{F}_n$ generated by a fixed number of random elements, in particular proving that when it is infinite index that it is almost always the free profinite group on countably many generators. Our work here complements theirs, as they have determined the structure of the random normal subgroup and we determine the structure of the quotient by this random normal subgroup.

The bulk of this paper is devoted to showing the existence of the measure μ_u of Theorem 1.1. Let $\mu_{u,n}$ be the distribution of our random group $X_{u,n}$. Since the basic opens in our topology are also closed, it is clear that if μ_u exists, then for any basic open U we have $\mu_u(U) = \lim_{n \to \infty} \mu_{u,n}(U)$. The argument for the existence of μ_u breaks into two major parts. The first part is to show the limit $\lim_{n \to \infty} \mu_{u,n}(U)$ exists. The second part is to show that these measures on basic opens define a countably additive measure. After giving some notation and basic definitions in Section 2, we will give the values of μ_u on basic opens in Section 3 for easy reference. Then in Section 4 we set up the strategy for proving $\lim_{n \to \infty} \mu_{u,n}(U)$ exists, which is entirely group theoretical. This argument will take us through Section 8. It is easy to express $\mu_{u,n}$ in group theory terms involving $\hat{F}_n$. However, such expressions do not allow one to take a limit as $n \to \infty$, and so the main challenge is to extract $\hat{F}_n$ from the description of the probabilities so that they only involve the number n and group theoretical quantities that do not depend on n. This requires several steps. In Section 5, we express the probabilities in terms of multiplicities of certain groups appearing in $\hat{F}_n$. In Section 6, we bound what possible groups can have positive multiplicities. In Section 7, we relate the multiplicities to a count of certain surjections, and finally in Section 8 we count these surjections in another way that eliminates $\hat{F}_n$ from our description of the probabilities.

The next challenge is to show the countable additivity of the μ_u that we have then defined on basic opens. It follows from Fatou's lemma that for a finite set S of finite groups,

$$\sum_{H \text{ is finite}} \lim_{n \to \infty} \mu_{u,n}(U_{S,H}) \leq 1.$$

However, a priori, this inequality may be strict. In the limit as n goes to infinity there could be escape of mass. To show that this does not occur, we require bounds on the $\mu_{u,n}(U_{S,H})$ that are sufficiently uniform in n. The difficultly is that our group theoretical expressions do not easily lend themselves to the kind of bounds useful for an analytic argument. We obtain the necessary uniformity by considering a notion of *chief factor pairs*, which generalizes the notion of a chief factor of a group to also include the conjugation action on the chief factor. We are able to bound the size of the outer action of conjugation on chief factors for a given S in Section 6, which then, combined with an induction on S, gives us the uniformity necessary to show in Section 9 that the above inequality is actually an equality. That is the heart of the proof of countable additivity, which we show in Section 9.

Once we have established the existence of the measure μ_u with the desired measure on basic opens, Theorem 1.1 follows immediately in Section 10. In Section 11, we give the measures of sets of the form $\{X \in \mathcal{P} \mid X^{\bar{S}} \simeq H^{\bar{S}}\}$ for arbitrary sets S of finite groups, and see that μ_u and $\lim_{n \to \infty} \mu_{u,n}$ agree there, giving a stronger convergence than the weak

convergence of Theorem 1.1. There, one inequality is automatic, and we then we argue that we either have the necessary uniformity to get equality, or that the larger probability is 0, which also gives equality. The result of Section 11 then allows us to compute measures of many different Borel sets, and in Section 12, we give many examples including the trivial group, infinite groups, and distributions of the abelianization and pro-nilpotent quotient. In Section 13, we see that the measures μ_u give positive measure to any basic open where groups can be generated by u more relations than generators. Finally, in Section 14, we compare the profinite model used in this paper to the discrete group model described above.

This is the beginning of investigation into these random groups, and there are many further questions we would like to understand. Are these measures universal in the sense of [Woo15], i.e. would we still get μ_u as $n \to \infty$ even if we took our relations from a different measure? Are these measures determined by their moments, which in [HB94, Lemma 18], [FK06, Section 4.2], [EVW16, Lemma 8.2], [Woo17, Theorem 8.3], and [BW17, Theorem 1.4] has been an important tool to identify analogous random groups? What is the measure of the set of all infinite groups when $u \geq 0$ (see Example 12.8, and note by [JL06] this implies the normal subgroup generated by the relations is free on countably many generators with probability 1)? What is the measure of the set of finitely generated groups, and of finitely presented groups? Do the $\mu_{u,n}$ converge strongly to μ_u? Besides their inherent interest, many of these questions have implications for the possible connections to number theory described above.

2. Notation and basic group theoretical definitions

2.1. **Notation.** In Section 15, we give a list of symbols used in the paper in more than one section for ease of reference.

Whenever we take a quotient by relations, we always mean by the closed, normal subgroup generated by those relations. For elements $x_1, \ldots$ of a group G, we write $[x_1, \ldots]_G$ for the closed normal subgroup of G generated by $x_1, \ldots$.

We write $G \simeq H$ to mean that G and H are isomorphic. For profinite groups, we always mean isomorphic as profinite groups. For two groups G and H, we write $G = H$ when there is an obvious map from one of G or H to the other (e.g. when H is defined as a quotient or subgroup of G) and that map is an isomorphism.

For a group G, we write G^j for the direct product of j copies of G. If H is a subgroup of G, then we denote the centralizer of H by $\mathbf{C}_G(H)$.

When we say a set of finite groups, we always mean a set of isomorphism classes of finite groups.

2.2. *F*-**groups.** If F is a group, an *F-group* is a group G with an action of F. A morphism of F-groups is a group homomorphism that respects the F-action. An F-subgroup is a subgroup G such that $f(G) = G$ for all $f \in F$, and an F-quotient is a group quotient homomorphism that respects the F-action. An *irreducible F-group* is an F-group with no normal F-subgroups except the trivial subgroup and the group itself. We write $\mathrm{Hom}_F(G_1, G_2)$ for the F-group morphisms from G_1 to G_2 and $h_F(G) := |\mathrm{Hom}_F(G, G)|$. We write $\mathrm{Sur}_F(G_1, G_2)$ for the F-group surjections from G_1 to G_2, and $\mathrm{Aut}_F(G)$ for the F-group automorphisms of G. For a sequence x_k in an F-group G, let $[x_1, \ldots]_F$ be the closed normal F-subgroup of G generated by the x_k.

2.3. H-extensions. For a group H, an H-*extension* is a group E with a surjective morphism $\pi : E \to H$. If $\pi : E \to H$ and $\pi' : E' \to H$ are H-extensions, a morphism from (E, π) to (E', π') is a group homomorphism $f : E \to E'$ such that $\pi = \pi' \circ f$. If $\pi : E \to H$ and $\pi' : E' \to H$ are H-extensions, we write $\mathrm{Sur}_H(\pi, \pi')$ for the set of surjective morphisms from (G, π) to (G', π'). For an H-extension E, we write $\mathrm{Aut}_H(E, \pi)$ for the automorphisms of (E, π) as an H-extension. If (E, π) is an H-extension, a sub-H-extension is a subgroup E' of E with $\pi|_{E'}$, such that $\pi|_{E'}$ is surjective. Note that when $\ker \pi$ is abelian, it is an H-group under conjugation in E.

2.4. Pro-$\bar{S}$ completions and level S groups. Given a set S of finite groups, we let $\bar{S}$ denote the smallest set of groups containing S that is closed under taking quotients, subgroups and finite direct products. (This is called the variety of groups generated by S.) Given a profinite group G, we write $G^{\bar{S}}$ for its pro-$\bar{S}$ completion, which is defined as

$$G^{\bar{S}} = \varprojlim_M G/M,$$

where the inverse limit is taken over all closed normal subgroups M of G such that $G/M \in \bar{S}$.

Definition. For a set S of finite groups, we say that a profinite group G is *level S* if $G \in \bar{S}$. Also, for a positive integer ℓ, let S_ℓ be the set consisting of all groups whose order is less than or equal to ℓ. Then we say G is *level ℓ* if $G \in \bar{S}_\ell$. Note that for $G \in \mathcal{P}$ we have that G is level S if and only if $G = G^{\bar{S}}$.

3. Definition of μ_u

For integers $n \geq 1$ and $u > -n$, recall that $X_{u,n}$ is the random group defined by taking quotient of the free profinite group $\hat{F}_n$ on n generators by $n+u$ independent random relations that are taken from the Haar measure on $\hat{F}_n$. For finite set S of finite groups and finite group H, let $U_{S,H} := \{X \in \mathcal{P} \,|\, X^{\bar{S}} \simeq H\}$ (where $\mathcal{P}$ is the set of isomorphism classes of profinite groups G such that the pro-$\bar{S}$ completion $G^{\bar{S}}$ is finite for all finite sets S of finite groups). We have a measure $\mu_{u,n}$ on the σ-algebra of Borel sets of $\mathcal{P}$ such that $\mu_{u,n}(A) = \mathrm{Prob}(X_{u,n} \in A)$. We will define a measure μ_u, for each integer u, at first as a measure on the algebra $\mathcal{A}$ of sets generated by the $U_{S,H}$. For $A \in \mathcal{A}$, we define

$$(3.1) \qquad\qquad \mu_u(A) := \lim_{n \to \infty} \mu_{u,n}(A).$$

We will below establish that 1) this limit exists when $A = U_{S,H}$ (see Theorem 8.1, and Equation (3.2) just below, in which we give the value of the limit), and hence for any $A \in \mathcal{A}$ since the limit is compatible with finite sums and subtraction from 1; and 2) μ_u is countably additive on $\mathcal{A}$ (see Theorem 9.1). These two results represent the bulk of the work of the paper. Then by Carathéodory's extension theorem, it follows that μ_u extends uniquely to a probability measure on $\mathcal{P}$.

3.1. Value of μ_u on basic open sets. Given a finite group H, let $\mathcal{A}_H$ be the set of isomorphism classes of non-trivial finite abelian irreducible H-groups. Let $\mathcal{N}$ be the set of isomorphism classes of finite groups that are isomorphic to G^j for some finite simple non-abelian group G and a positive integer j. Let S be a set of finite groups, and H a finite level

S group. For $G \in \mathcal{A}_H$, we define the quantity

$$\lambda(S, H, G) := (h_H(G) - 1) \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E, \pi) \\ \text{such that } \ker \pi \simeq G \text{ as } H\text{-groups}, \\ \text{and } E \text{ is level } S}} \frac{1}{|\operatorname{Aut}_H(E, \pi)|}.$$

We will see in Remark 8.13 that for $G \in \mathcal{A}_H$, the number $\lambda(S, H, G)$ is an integer power of $h_H(G)$. If $G \in \mathcal{N}$, we define

$$\lambda(S, H, G) := \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E, \pi) \\ \text{such that } \ker \pi \simeq G^j \text{ as groups}, \\ \ker \pi \text{ irred. } E\text{-group}, \\ \text{and } E \text{ is level } S}} \frac{1}{|\operatorname{Aut}_H(E, \pi)|}.$$

The definitions are not quite parallel in the abelian and non-abelian cases, but this is un-avoidable given the different behavior of abelian and non-abelian simple groups.

It will follow from Theorem 8.1 below that for a finite set S of finite groups and a finite level S group H, we have

$$(3.2) \quad \mu_u(U_{S,H}) = \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{G \in \mathcal{A}_H} \prod_{i=0}^{\infty} (1 - \lambda(S, H, G) \frac{h_H(G)^{-i-1}}{|G|^u}) \prod_{G \in \mathcal{N}} e^{-|G|^{-u}\lambda(S,H,G)}.$$

Theorem 11.4 gives the analogous result for an infinite set S. We will see in Section 6 that for finite S only finitely many elements of $\mathcal{A}_H$ and $\mathcal{N}$ contribute non-trivially to this product.

4. Setup and organization of the proofs

The proof of Equation (3.2) will be established from Section 5 to Section 8, which are dominated by group theoretical methods. Here we outline the proof for the reader's convenience.

Suppose n is a positive integer, S is a finite set of finite groups, and H is a finite level S group. Then $(\hat{F}_n)^{\bar{S}}$ is a finite group [Neu67, Cor. 15.72] and $(X_{u,n})^{\bar{S}}$ has the same distribution as the quotient of $(\hat{F}_n)^{\bar{S}}$ by $n + u$ independent, uniform random relations $r_1, \cdots r_{n+u}$ from $(\hat{F}_n)^{\bar{S}}$. By the definition of μ_u, we have that

$$\mu_u(U_{S,H}) = \lim_{n \to \infty} \operatorname{Prob}((\hat{F}_n)^{\bar{S}}/[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}} \simeq H).$$

We consider a normal subgroup N of $(\hat{F}_n)^{\bar{S}}$ with an isomorphism $(\hat{F}_n)^{\bar{S}}/N \simeq H$. Let M be the intersection of all maximal proper $(\hat{F}_n)^{\bar{S}}$-normal subgroups of N. We denote $F = (\hat{F}_n)^{\bar{S}}/M$ and $R = N/M$. Then for independent, uniform random elements $r_1, \cdots, r_{n+u}$ of $(\hat{F}_n)^{\bar{S}}$, we have that $[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}} = N$ if and only if R is the normal subgroup generated by the images of $r_1, \cdots, r_{n+u}$ in F. Indeed, the "only if" direction is clear; and if $[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}}/M = R$, then $[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}} = N$ since $[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}}$ being contained in a proper maximal $(\hat{F}_n)^{\bar{S}}$-normal subgroup of N would imply that its image is contained in a proper maximal F-normal subgroup of R.

Any two surjections from $(\hat{F}_n)^{\bar{S}}$ to H are isomorphic as H-extensions [Lub01, Proposition 2.2]. Thus, the short exact sequence

$$(4.1) \qquad\qquad 1 \to R \to F \to H \to 1$$

does not depend (up to isomorphisms of F as an H-extension) on the choice of the normal subgroup N.

Definition. Given a finite set S of finite groups, a positive integer n and a finite level S group H, the short exact sequence defined in Equation (4.1) is called *the fundamental short exact sequence associated to S, n and H.*

By the above arguments, $\mathrm{Prob}((\hat{F}_n)^{\bar{S}}/[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}} \simeq H)$ equals the number of normal subgroups N of $(\hat{F}_n)^{\bar{S}}$ with $(\hat{F}_n)^{\bar{S}}/N \simeq H$ times the probability that independent, uniform random elements $x_1, \cdots, x_{n+u} \in F$ normally generate R. Note that the number of such normal subgroups N is $|\mathrm{Sur}((\hat{F}_n)^{\bar{S}}, H)|/|\mathrm{Aut}(H)|$, and there is a one-to-one correspondence between $\mathrm{Sur}((\hat{F}_n)^{\bar{S}}, H)$ and $\mathrm{Sur}(\hat{F}_n, H)$. It follows that

$$(4.2) \quad \mathrm{Prob}((\hat{F}_n)^{\bar{S}}/[r_1, \cdots, r_{n+u}]_{(\hat{F}_n)^{\bar{S}}} \simeq H) = \frac{|\mathrm{Sur}(\hat{F}_n, H)|}{|\mathrm{Aut}(H)|} \mathrm{Prob}([x_1, \cdots, x_{n+u}]_F = R).$$

It therefore suffices to compute $\mathrm{Prob}([x_1, \cdots, x_{n+u}]_F = R)$. Note that R is an F-group under the conjugation action. It will follow from Lemma 5.11 that R is a direct product of irreducible F-groups. Theorem 5.1 will prove the formula for $\mathrm{Prob}([x_1, \cdots, x_{n+u}]_F = R)$ for F and R where R is a direct product of irreducible F-groups, in terms of the multiplicities of the various irreducible F-group factors of R. In Section 6, we will give some criteria for which irreducible F-groups can appear in R. Then in Section 7, we will relate the multiplicities of irreducible factors in R to the number of normal subgroups of R with specified quotients. In Section 8, we will count these normal subgroups of R in another way in order to finally give an explicit formula for $\mu_{u,n}(U_{S,H})$. This formula will be explicit enough that we can easily take the limit as $n \to \infty$, giving Equation (3.2).

5. Generating probabilities for products of irreducible F-groups

Throughout this section, we let $n \geq 1$ and $u > -n$ be integers, F a group, and R a finite product of finite irreducible F-groups. (We don't require R to be a subgroup of F.) The goal of this section is to prove the following theorem which gives the probability that the normal F-subgroup generated by $n + u$ random elements of R is the whole group.

Theorem 5.1. *Let F be a group and G_i be finite irreducible F-groups for $i = 1, \ldots, k$ such that for $i \neq j$, we have that G_i and G_j are not isomorphic F-groups, and let m_i be non-negative integers. Let $R = \prod_{i=1}^{k} G_i^{m_i}$. Then*

$$\mathrm{Prob}([x_1, \ldots, x_{n+u}]_F = R) = \prod_{\substack{1 \leq i \leq k \\ G_i\ abelian}} \prod_{j=0}^{m_i-1} (1 - h_F(G_i)^j |G_i|^{-n-u}) \prod_{\substack{1 \leq i \leq k \\ G_i\ non\text{-}abelian}} (1 - |G_i|^{-n-u})^{m_i}$$

where the x_i are independent, uniform random elements of R.

Remark 5.2. Given a finite abelian irreducible F-group G, if we let $\mathfrak{m}$ be maximal such that $G^{\mathfrak{m}}$ can be generated by one element as an F-group, then we have $h_F(G)^{\mathfrak{m}} = |G|$. This follows from Theorem 5.1 because if we take $m_i = \mathfrak{m}$, the probability that one element generates G^{m_i} is positive, but if we take $m_i = \mathfrak{m} + 1$ the probability is 0.

7

We will build up to Theorem 5.1 through several lemmas. First, we determine the structure of normal F-subgroups of products of irreducible F-groups.

Lemma 5.3. *If G_i are irreducible F-groups and N is an F-subgroup of $\prod_{i=1}^{m} G_i$ that projects to 1 or G_i in each factor, then there exists a subset $J \subset \{1, \ldots, m\}$ such that the projection of N to $\prod_{i \in J} G_i$ is an isomorphism.*

Proof. We prove this by induction on m. Let π_m be the projection map from $\prod_{i=1}^{m} G_i$ to G_m, and π the projection map from N to $\prod_{i=1}^{m-1} G_i$. Since $\pi_m(N)$ is 1 or G_m, and $\pi_m(\ker \pi)$ is a normal F-subgroup of $\pi_m(N)$, we have $\pi_m(\ker \pi)$ is 1 or G_m. If $\pi_m(\ker \pi) = 1$, then since $\ker \pi \cap \ker \pi_m = 1$, we have $\ker \pi = 1$ and N is isomorphic to $\pi(N)$. If $\pi_m(\ker \pi) = G_m$, then N is isomorphic to $\pi(N) \times G_m$. In either case, we apply the inductive hypothesis to $\pi(N)$ and conclude the lemma. $\qquad\square$

Lemma 5.4. *Let G_1 and G_2 be irreducible F-groups. Then any homomorphism of F-groups $\phi : G_1 \to G_2$ with normal image is either trivial or an isomorphism.*

Proof. If it is not trivial, then $\ker(\phi)$ is a normal F-subgroup and so must be trivial, and $\operatorname{im}(\phi)$ is a normal F-subgroup and must be G_2, so it is a bijection. $\qquad\square$

Lemma 5.5. *Let G_i be irreducible F-groups for $i = 1, \ldots, k$ such that for $i \neq j$, we have that G_i and G_j are not isomorphic as F-groups. Let N be a normal F-subgroup of $\prod_{i=1}^{k} G_i^{m_i}$, then $N = \prod_{i=1}^{k} N_i$, where N_i is a normal F-subgroup of $G_i^{m_i}$.*

Proof. Since N is a normal F-subgroup of $\prod_{i=1}^{k} G_i^{m_i}$, its projection to each factor G_i is normal F-subgroup of G_i, hence it's either 1 or G_i. By Lemma 5.3, we can write N abstractly as $\prod_{i=1}^{k} G_i^{n_i}$ and define N_i to be the subgroup of N such that it is the image of the factor $G_i^{n_i}$ under the chosen isomorphism between $\prod_{i=1}^{k} G_i^{n_i}$ and N. From Lemma 5.4, we see that for $i \neq j$ the projection $N_i \to G_j^{m_j}$ is trivial, and it follows that N_i is the subgroup of elements of N that are trivial in the projections to $G_j^{m_j}$ for all $j \neq i$. Finally, if $n \in N_i$, then we can see that any $\prod_{i=1}^{k} G_i^{m_i}$ conjugate of n is trivial in the projections to $G_j^{m_j}$ for all $j \neq i$ and in is N. Hence N_i is a normal F-subgroup of $G_i^{m_i}$. $\qquad\square$

The followings are two corollaries of Lemma 5.5.

Corollary 5.6. *Let G_i be irreducible F-groups for $i = 1, \ldots, k$ such that for $i \neq j$, we have that G_i and G_j are not isomorphic as F-groups. Let N be a normal F-subgroup of $\prod_{i=1}^{k} G_i^{m_i}$. Then $N = \prod_{i=1}^{k} G_i^{m_i}$ if and only if $\pi_i(N) = G_i^{m_i}$ for each projection $\pi_i : N \to G_i^{m_i}$.*

Corollary 5.7. *Let G_i be finite irreducible F-groups for $i = 1, \ldots, k$ such that for $i \neq j$, we have that G_i and G_j are not isomorphic as F-groups, and let m_i be non-negative integers. Let $R = \prod_{i=1}^{k} G_i^{m_i}$. Then*

$$\operatorname{Prob}([x_1, \ldots, x_{n+u}]_F = R) = \prod_{i=1}^{m} \operatorname{Prob}([y_{i,1}, \ldots, y_{i,n+u}]_F = G_i^{m_i}),$$

where the x_k are independent, uniform random elements of R, and the $y_{i,k}$ are independent, uniform random elements of $G_i^{m_i}$.

The next lemma will help us determine when $[y_{i,1}, \ldots, y_{i,n+u}]_F = G_i^{m_i}$.

Lemma 5.8. *Let G be an irreducible F-group. If G is non-abelian, then a normal F-subgroup N of G^m is all of G^m if and only if it is non-trivial in each of the m projections to G. If G is abelian, then a normal F-subgroup N of G^m is all of G^m if and only if the projection onto the product of the first $m-1$ factors is surjective and the projection of N onto the mth factor does not factor through the projection onto the product of the first $m-1$ factors.*

Proof. The only if direction is clear. We let π be the projection of N onto the first $m-1$ factors of G^m and π_m the projection onto the last factor. For the other direction, for non-abelian G we induct and so we have by the inductive hypothesis $\pi(N) = G^{m-1}$. For G abelian we have $\pi(N) = G^{m-1}$ as a hypothesis. We consider $\pi_m(\ker \pi)$, which must be 1 or G. If $\pi_m(\ker \pi)$ is G, then we see $N = G^m$, as it includes element with every possible first $m-1$ coordinates, and then an element with trivial first $m-1$ coordinates and every possible mth coordinate. Now we show that we cannot have $\pi_m(\ker \pi) = 1$. Suppose for the sake of contradiction that $\pi_m(\ker \pi) = 1$. Then since $\ker \pi_m \cap \ker \pi = 1$, we have $\ker \pi = 1$, and π is an isomorphism on N, and in particular π_m factors through π. So given our hypotheses, this can only happen when G is non-abelian. We write elements $(a, b) \in G^{m-1} \times G$. Since $\pi_m(N)$ is non-trivial, it must be G by the irreducibility of G. For every $b \in G$, we have some $a \in G^{m-1}$ such that $(a, b) \in N$. However, since N is normal, that means $(a, gbg^{-1}) \in N$ for every $g \in G$. Since π_m factors through π, we have that $b = gbg^{-1}$ for every $b, g \in G$, which is a contradiction, since above we saw we can only be in this case if G is non-abelian. $\square$

Lemma 5.8 lets us compute the probabilities appearing in the right-hand side of Corollary 5.7 in the following two corollaries.

Corollary 5.9. *If G is a finite non-abelian irreducible F-group, and y_k for $k = 1, \ldots, n+u$ are independent, uniform random elements of G^m, then*

$$\mathrm{Prob}([y_1, \ldots, y_{n+u}]_F = G^m) = (1 - |G|^{-n-u})^m.$$

Corollary 5.10. *If G is a finite abelian irreducible F-group, and y_k for $k = 1, \ldots, n+u$ are independent, uniform random elements of G^m, then*

$$\mathrm{Prob}([y_1, \ldots, y_{n+u}]_F = G^m) = \prod_{k=0}^{m-1}(1 - h_F(G)^k|G|^{-n-u}).$$

Proof. Let π_k be the projection of G^m onto the kth factor, and Π_k the projection of G^m to the first k factors. We have

$$\mathrm{Prob}([y_1, \ldots, y_{n+u}]_F = G^m)$$

$$= \prod_{k=0}^{m-1} \mathrm{Prob}(\Pi_{k+1}([y_1, \ldots, y_{n+u}]_F) = G^{k+1} \mid \Pi_k([y_1, \ldots, y_{n+u}]_F) = G^k).$$

We condition on the values of $\Pi_k(y_i)$, and we still have, with this conditioning, that the $\pi_{k+1}(y_i)$ are uniform, independent random in G. By Lemma 5.8, given $\Pi_k([y_1, \ldots, y_{n+u}]_F) = G^k$, we will have $\Pi_{k+1}([y_1, \ldots, y_{n+u}]_F) = G^{k+1}$, exactly if the map $\pi_{k+1}|_{[y_1, \ldots, y_{n+u}]_F}$ does not factor through $\Pi_k|_{[y_1, \ldots, y_{n+u}]_F}$. We have a total of $|G|^{n+u}$ choices for the $(n+u)$-tuple $(\pi_{k+1}(y_1), \cdots, \pi_{k+1}(y_{n+u}))$. Call choice for $(\pi_{k+1}(y_1), \ldots, \pi_{k+1}(y_{n+u}))$ *bad* if $\pi_{k+1}|_{[y_1, \ldots, y_{n+u}]_F}$ factors through $\Pi_k|_{[y_1, \ldots, y_{n+u}]_F}$. Since $\Pi_k([y_1, \ldots, y_{n+u}]_F) = G^k$, there are $|\mathrm{Hom}_F(G^k, G)|$ choices for maps from G^k to G, each of which gives a bad choice for $(\pi_{k+1}(y_1), \ldots, \pi_{k+1}(y_{n+u}))$

(and all bad choices arise this way). For two maps in $\mathrm{Hom}_F(G^k, G)$ to give the same bad choice, they would have to agree on $\Pi_k(y_i)$ for all i, and since $\Pi_k([y_1, \ldots, y_{n+u}]_F) = G^k$, this would imply the two maps in $\mathrm{Hom}_F(G^k, G)$ would be the same. Thus there are $|\mathrm{Hom}_F(G^k, G)|$ bad choices in $|G|^{n+u}$ for the $\pi_{k+1}(y_i)$, and as $|\mathrm{Hom}_F(G^k, G)| = h_F(G)^k$, the corollary follows. $\qquad \square$

Theorem 5.1 now follows from Corollaries 5.7, 5.9, and 5.10. Also, we can now prove the following lemma which is key for our general approach in Section 4.

Lemma 5.11. *Let G be a finite group, and let N be a normal subgroup of G. Let M be the intersection of all maximal proper, G-normal subgroups of N. Then N/M is a G/M-group under the action of conjugation. We have that N/M is isomorphic, as an G/M-group, to a direct product of irreducible G/M-groups. Moreover, among these irreducible G/M-groups, the abelian ones all have the action of G/M factor through G/N, so are also irreducible G/N-groups.*

Proof. We consider N as a G-group under conjugation. A subgroup of N is a normal subgroup of G if and only if it is a G-subgroup of N. Taking the quotient modulo M gives us a containment respecting bijection between the G-subgroups of N containing M and the G/M-subgroups of N/M. Since all maximal proper G-subgroups of N contain M, the quotient map gives us a bijection between the maximal proper G-subgroups of N and the maximal proper G/M-subgroups of N/M, and in particular the quotient $M/M = 1$ is the quotient of all the maximal proper G/M-subgroups of N/M. Let M_i be the maximal proper G/M-subgroups of N/M. Each $(N/M)/M_i$ is an irreducible G/M-group. We have that N/M is a subgroup of $\prod_i (N/M)/M_i$ that surjects into each factor, N/M is isomorphic to a direct product of irreducible G/M-groups by Lemma 5.3. On an abelian irreducible G/M-group factor, conjugation by any element in N/M gives the trivial group action, so we have the last statement of the lemma. $\qquad \square$

6. Determining factors appearing in R

Throughout this section, we assume S is a set of finite groups, n is a positive integer, and H is a finite level S group. If S is finite, then we let

$$1 \to R \to F \to H \to 1$$

be the fundamental short exact sequence associated to S, n and H (see Section 4). In this section, we will bound which irreducible F-groups are possible factors in R. A finite irreducible F-group is characteristically simple (that is, it contains no proper nontrivial characteristic subgroups) and thus, as a group, a direct product Γ^m of isomorphic simple groups. First, when the group H is fixed, Lemma 6.1 will bound the possible power m for factors in R. For fixed S, Corollary 6.12 will then bound the possible simple group Γ for factors in R. We take a slightly longer than necessary route to Corollary 6.12 because along the way we will develop the technology to prove Corollary 6.13, which will later be critical in Section 9 for our proof of countable additivity of μ_u.

Lemma 6.1. *Let (E, π) be an H-extension such that $G = \ker \pi$ is a finite irreducible E-group. Then G is isomorphic to Γ^m for some finite simple group Γ and $m \le |H|$.*

Proof. Let $G \simeq \Gamma^m$, where Γ is a finite simple group. If $\Gamma = \mathbb{Z}/p\mathbb{Z}$, then $G \subset \mathbf{C}_E(G)$ and the map $H \to \mathrm{Aut}(G) = \mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ defined by conjugation action is an irreducible representation of H. Since for any non-zero vector $v \in \mathbb{F}_p^m$, the vectors hv, for $h \in H$, span a subrepresentation of H, we have the dimension m is at most $|H|$.

If Γ is non-abelian, then consider an embedding $\iota : \Gamma \hookrightarrow \Gamma^m$ such that the image is a normal subgroup. There is an element $a = (a_1, \cdots, a_m) \in \iota(\Gamma)$ such that a_i is not the identity element for some i. Let $b \in \Gamma^m$ have jth coordinate 1 for $j \neq i$ and ith coordinate $\gamma \in \Gamma$. Then since $\iota(\Gamma)$ is normal, we have that the commutator $[a, b] \in \iota(\Gamma)$. The element $[a, b]$ is trivial in all but the ith coordinate, where it is $[a_i, \gamma]$. So the intersection of $\iota(\Gamma)$ and the ith factor (which is a normal subgroup of Γ) contains $[a_i, \gamma]$ for some non-trivial $a_i \in \Gamma$ and all $\gamma \in \Gamma$. Since Γ is a non-abelian simple group, this means the intersection of $\iota(\Gamma)$ and the ith factor is non-trivial, and hence all of the ith factor. So $\iota(\Gamma)$ is exactly the ith factor of Γ^m. We have thus showed that a normal subgroup of Γ^m that is isomorphic to Γ must be one of the m factors. So we have a well-defined map $\mathrm{Aut}(\Gamma^m) \to S_m$ (the symmetric group on m elements), and note that $\mathrm{Inn}(\Gamma^m)$ is in the kernel of this map. If Γ^m is an irreducible E-group, the action of H on the factors must be transitive, which proves $m \leq |H|$. $\qquad\square$

Recall that a chief series of a finite group G is a chain of normal subgroups

(6.2) $$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$$

such that for each $0 \leq i \leq r - 1$, G_i is normal in G and the quotient group G_{i+1}/G_i is a minimal normal subgroup of G/G_i. If M is a minimal normal subgroup of G, then define ρ_M to be the homomorphism

$$\begin{aligned} \rho_M : G &\to \mathrm{Aut}(M) \\ g &\mapsto (x \mapsto gxg^{-1})_{x \in M}. \end{aligned}$$

The kernel of ρ_M is the centralizer $\mathbf{C}_G(M)$ of M in G. So ρ_M gives an isomorphism from $G/\mathbf{C}_G(M)$ to the subgroup $\rho_M(G)$ of $\mathrm{Aut}(M)$. In fact, since M is a minimal normal subgroup of G, it is a direct product of isomorphic simple groups. If M is a direct product of isomorphic abelian simple groups, i.e. an elementary abelian p-group, then $\rho_M(M) = \mathrm{Inn}(M) = 1$; otherwise, $\rho_M(M) = \mathrm{Inn}(M) \simeq M$. Thus, $\mathrm{Inn}(M)$ is always a normal subgroup of $\rho_M(G)$ and $\rho_M(G)/\mathrm{Inn}(M) \simeq G/(M \cdot \mathbf{C}_G(M))$.

Definition. A *chief factor pair* is a pair of finite groups (M, A) such that M is an irreducible A-group and the A-action on M is faithful (hence A is naturally a subgroup of $\mathrm{Aut}(M)$). In particular, the chief series (6.2) gives a sequence of chief factor pairs $(G_{i+1}/G_i, \rho_{G_{i+1}/G_i}(G/G_i))$, and we call them *chief factor pairs of the series (6.2)*.

Definition. Two chief factor pairs (M_1, A_1) and (M_2, A_2) are *isomorphic* if there exists an isomorphism $\alpha : M_1 \to M_2$ such that the induced isomorphism $\alpha^* : \mathrm{Aut}(M_1) \to \mathrm{Aut}(M_2)$ maps A_1 to A_2.

The following is an analog of the Jordan-Hölder Theorem.

Lemma 6.3. *Let G be a finite group. Suppose there are two chief series of G:*

(6.4) $$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$$

11

$$\text{and}\quad 1 = I_0 \lhd I_1 \lhd \cdots \lhd I_s = G.$$

Then

    (1) $r = s$;

    (2) the list of isomorphism classes of chief factor pairs $\left\{ \left(G_{i+1}/G_i, \rho_{G_{i+1}/G_i}(G/G_i) \right)_{i=0}^{r-1} \right\}$

    is a rearrangement of the list $\left\{ \left(I_{i+1}/I_i, \rho_{I_{i+1}/I_i}(G/I_i) \right)_{i=0}^{s-1} \right\}$.

Proof. We prove this by induction on $|G|$. The case that $|G| = 1$ is trivial. Assume the lemma is true for all groups of order less than k and G is a group of order k. If $G_1 = I_1$ then

$$1 \lhd G_2/G_1 \lhd \cdots \lhd G_r/G_1 = G/G_1$$
$$\text{and}\quad 1 \lhd I_2/I_1 \lhd \cdots I_s/I_1 = G/I_1$$

are two chief series of G/G_1. So the lemma is proved for G by the induction hypothesis.

    Assume $G_1 \neq I_1$. Since they are minimal normal subgroups, $G_1 \cap I_1 = 1$ and $G_1 I_1 = G_1 \times I_1$. Define J_2 to be the product $G_1 I_1$. Then $J_2/G_1 \simeq I_1$ is a minimal normal subgroup of G/G_1 and we can construct a chief series of G passing through G_1 and J_2

(6.6) $$1 \lhd G_1 \lhd J_2 \lhd J_3 \lhd \cdots \lhd J_t = G.$$

Comparing chief series (6.4) and (6.6), it follows by the inductive hypothesis for the group G/G_1 that $r = t$ and

(6.7) $\left\{ \left(G_{i+1}/G_i, \rho_{G_{i+1}/G_i}(G/G_i) \right)_{i=0}^{r-1} \right\} \sim \left\{ \left(G_1, \rho_{G_1}(G) \right), \left(J_2/G_1, \rho_{J_2/G_1}(G/G_1) \right),$
$$\left(J_{i+1}/J_i, \rho_{J_{i+1}/J_i}(G/J_i) \right)_{i=2}^{t-1} \right\}$$

where the symbol $\sim$ means "is a rearrangement of". Let π be the quotient map $G \to G/G_1$. As $G_1 \lhd \mathbf{C}_G(I_1)$, if an element in G centralizes I_1, then its image under π centralizes $\pi(I_1) = J_2/G_1$. It follows that $\pi(\mathbf{C}_G(I_1)) \subseteq \mathbf{C}_{G/G_1}(J_2/G_1)$. Conversely, if a is an element in G such that $\pi(a) \in \mathbf{C}_{G/G_1}(J_2/G_1)$, then for every $h \in I_1$, we have $\pi(aha^{-1}) = \pi(h)$, which indicates that there exists $g \in G_1$ such that $aha^{-1} = hg$. But $I_1 \lhd G$, so $aha^{-1} \in I_1$. It follows from $I_1 \cap G_1 = 1$ that $g = 1$, and hence $a \in \mathbf{C}_G(I_1)$, which proves $\pi(\mathbf{C}_G(I_1)) = \mathbf{C}_{G/G_1}(J_2/G_1)$. Thus we have

$$G\big/\mathbf{C}_G(I_1) \;\cong\; G/G_1\big/\mathbf{C}_G(I_1)/G_1$$
$$\cong\; G/G_1\big/\mathbf{C}_{G/G_1}(J_2/G_1).$$

Therefore the chief factor pairs $\left(I_1, \rho_{I_1}(G) \right)$ and $\left(J_2/G_1, \rho_{J_2/G_1}(G/G_1) \right)$ are isomorphic. So the list (6.7) is

(6.8) $$\sim \left\{ \left(G_1, \rho_{G_1}(G) \right), \left(I_1, \rho_{I_1}(G) \right), \left(J_{i+1}/J_i, \rho_{J_{i+1}/J_i}(G/J_i) \right)_{i=2}^{t-1} \right\}.$$

Similarly, by comparing the following chief series of G

(6.9) $$1 \lhd I_1 \lhd J_2 \lhd J_3 \lhd \cdots \lhd J_t = G.$$

with (6.5), we finish the proof of the lemma. $\qquad\square$

Definition. If G is a finite group, then define $\mathcal{CF}(G)$ to be the set consisting of all isomorphism classes of chief factor pairs of a chief series of G ($\mathcal{CF}(G)$ does not depend on the choice of chief factor series by Lemma 6.3). If T is a set of finite groups, then

$$\mathcal{CF}(T) := \bigcup_{G \in T} \mathcal{CF}(G).$$

The following lemma shows that every factor in R comes from $\mathcal{CF}(\bar{S})$.

Lemma 6.10. *Let S be a finite set of finite groups, and R, F and H as defined at the beginning of this section. If G is an irreducible F-subgroup of R, then $(G, \rho_G(F)) \in \mathcal{CF}(\bar{S})$ and $\rho_G(F)/\operatorname{Inn}(G)$ is isomorphic to a quotient of H.*

Proof. Since F is a finite level S group and G is a minimal normal subgroup of F, we have $(G, F/\mathbf{C}_F(G)) \in \mathcal{CF}(\bar{S})$. Further, R is a direct product of irreducible F-groups, so R is contained in $\mathbf{C}_F(G) \cdot G$ and it follows that $(F/\mathbf{C}_F(G))/\operatorname{Inn}(G) = F/(\mathbf{C}_F(G) \cdot G)$ is a quotient of H. $\qquad \square$

In the rest of this section, we will bound the size of chief factor pairs.

Lemma 6.11. *If S is a set of finite groups that is closed under taking subgroups and quotients, then $\mathcal{CF}(\bar{S}) = \mathcal{CF}(S)$.*

Proof. Since $\bar{S}$ is the closure of S under taking finite direct products, quotients and subgroups, it suffices to show that none of these three actions creates new chief factor pairs not belonging to $\mathcal{CF}(S)$.

First, taking direct products and quotients does not create new chief factor pairs. If G and J are finite groups with chief series $1 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$ and $1 \triangleleft J_1 \triangleleft \cdots \triangleleft J_s = J$. Then the following chief series of $G \times J$

$$1 \triangleleft G_1 \times 1 \triangleleft \cdots G \times 1 \triangleleft G \times J_1 \triangleleft \cdots \triangleleft G \times J$$

implies that $\mathcal{CF}(G \times J) = \mathcal{CF}(G) \cup \mathcal{CF}(J)$. If N is a normal subgroup of G, then $\mathcal{CF}(G/N) \subseteq \mathcal{CF}(G)$ since we can always find a chief series of G passing through G/N.

Finally, assume J is a subgroup of G for $G \in \bar{S}$ such that $\mathcal{CF}(G) \subseteq \mathcal{CF}(S)$. We want to prove $\mathcal{CF}(J) \subseteq \mathcal{CF}(S)$. Let $1 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$ be a chief series of G. We can construct a chief series of J that passes through $G_i \cap J$ for every $i = 1, \cdots, r$. The chief factor pairs achieved from the elements between $G_i \cap J$ and $G_{i+1} \cap J$ are achieved from the group $J/(G_i \cap J) \simeq (J \cdot G_i)/G_i$, which is a subgroup of G/G_i. Thus it's enough to consider the positions between 1 and $G_1 \cap J$. Since $(G_1, \rho_{G_1}(G)) \in \mathcal{CF}(G) \subseteq \mathcal{CF}(S)$, there is a group $G' \in S$ and a minimal subgroup G'_1 of G' such that the chief factors $(G_1, \rho_{G_1}(G))$ and $(G'_1, \rho_{G'_1}(G'))$ are isomorphic, i.e. $\exists\, \alpha : G_1 \overset{\sim}{\to} G'_1$ such that $\alpha^* : \operatorname{Aut}(G_1) \overset{\sim}{\to} \operatorname{Aut}(G'_1)$ maps $\rho_{G_1}(G)$ to $\rho_{G'_1}(G')$. Define $A := \rho_{G_1}(J) = (J \cdot \mathbf{C}_G(G_1))/\mathbf{C}_G(G_1)$ that is a subgroup of $\rho_{G_1}(G)$. Note that the action of A on G_1 actually stabilizes $G_1 \cap J$. Let $J' := \rho_{G'_1}^{-1}(\alpha^*(A))$ and $J'_1 = \alpha(G_1 \cap J)$. So J' is a subgroup of G' satisfying the following short exact sequence

$$1 \to \mathbf{C}_{G'}(G'_1) \to J' \to \alpha^*(A) \to 1.$$

and J'_1 is a subgroup of $G'_1 \cap J'$.

Since $\mathbf{C}_{G'}(G'_1) \leq \mathbf{C}_{J'}(G'_1 \cap J')$, the action of J' via conjugation on $G'_1 \cap J'$ factors through $\alpha^*(A)$. Also, since the $\alpha^*(A)$ action on G'_1 stabilizes J'_1, we have that J'_1 is a normal subgroup

13

of J'. Because $G_1 \cap J$ with the action of A is isomorphic to J_1' with the action of $\alpha^*(A)$, every chief factor pair of G achieved from positions between 1 and $G_1 \cap J$ is also a chief factor pair of J' achieved via a series passing through J_1'. Finally, J' as a subgroup of G' belongs to S, so $\mathcal{CF}(J) \subseteq \mathcal{CF}(S)$ and we prove the lemma.

$\square$

Corollary 6.12. *If S is a set of finite groups, and $\Gamma \in \bar{S}$ is a simple group, then Γ is in the closure of S under taking subgroups and quotients.*

Proof. If $\Gamma \in \bar{S}$ is a simple group, then $(\Gamma, \text{Inn}(\Gamma)) \in \mathcal{CF}(\bar{S})$. By Lemma 6.11, Γ is in the closure of S under taking subgroups and quotients. $\square$

Corollary 6.13. *Let S be a finite set of finite groups. Then $\mathcal{CF}(\bar{S})$ is a finite set. Moreover, if ℓ is the upper bound of the orders of groups in S, then for any pair $(M, A) \in \mathcal{CF}(\bar{S})$, the quotient $A/\text{Inn}(M)$ is of level $\ell - 1$.*

Proof. Without lost of generality, let's assume S is closed under taking subgroups and quotients. By Lemma 6.11, $\mathcal{CF}(\bar{S}) = \mathcal{CF}(S)$ is finite, and for any chief factor pair $(M, A) \in \mathcal{CF}(\bar{S})$, there is a group $G \in S$ such that $(M, A) \in \mathcal{CF}(G)$. If M is abelian, then $|M||A| \leq |G| \leq \ell$; otherwise, M is non-abelian and $|A| = |M||A/\text{Inn}(M)| \leq |G| \leq \ell$. In either case, we have $|A/\text{Inn}(M)| \leq \frac{\ell}{2} \leq \ell - 1$. $\square$

Remark 6.14. The statement in Corollary 6.13 remains true if $\ell - 1$ is replaced by $\lfloor \ell/2 \rfloor$ but we will not use that stronger statement.

7. Counting maximal quotients of irreducible F-groups

In order to apply Theorem 5.1 to a group that we know, abstractly, to be a product of irreducible F-groups, we need to know the multiplicities of the various irreducible F-groups in the product. In this section, we relate those multiplicities to a count of surjections.

Theorem 7.1. *Let G_i be finite irreducible F-groups for $i = 1, \ldots, k$ such that G_i and G_j are not isomorphic for $i \neq j$. Then if G_j is abelian*

$$\# \text{Sur}_F \left(\prod_{i=1}^{k} G_i^{m_i}, G_j \right) = h_F(G_j)^{m_j} - 1$$

and if G_j is non-abelian

$$\# \text{Sur}_F \left(\prod_{i=1}^{k} G_i^{m_i}, G_j \right) = m_j |\text{Aut}_F(G_j)|.$$

This theorem follows immediately from Lemma 5.4 and the following lemmas.

Lemma 7.2. *Let G_i be finite irreducible F-groups for $i = 1, \ldots, k$ such that for $i \neq j$, we have that G_i and G_j are not isomorphic. The restriction map*

$$\text{Sur}_F \left(\prod_{i=1}^{k} G_i^{m_i}, G_j \right) \to \text{Hom}_F \left(G_j^{m_j}, G_j \right)$$

is a bijection to $\text{Sur}_F \left(G_j^{m_j}, G_j \right) \subset \text{Hom}_F \left(G_j^{m_j}, G_j \right)$.

14

Proof. Note that in a surjection, each G_i must go to a normal subgroup of G_j, and so by Lemma 5.4 the restriction to every G_i factor for $i \neq j$ is trivial. So that proves the above restriction map is injective. The restriction map is surjective to $\mathrm{Sur}_F\left(G_j^{m_j}, G_j\right)$ since $G_j^{m_j}$ is a quotient of $\prod_{i=1}^k G_i^{m_i}$. $\square$

Lemma 7.3. *Let G be a finite irreducible F-group and m a positive integer. We have*

$$\mathrm{Hom}_F(G^m, G) \subset \mathrm{Hom}_F(G, G)^m$$

by restriction to each factor. If G is abelian, then this inclusion is an equality. If G is non-abelian, then we have that $\mathrm{Hom}_F(G^m, G)$ is the subset of the m-tuples $\mathrm{Hom}_F(G, G)^m$ where at most 1 coordinate is a non-trivial morphism in $\mathrm{Hom}_F(G, G)$. The only homomorphism that is not surjective among those above is the trivial morphism.

Proof. If G is abelian, then for $\phi_i \in \mathrm{Hom}_F(G, G)$, we have a morphism $\phi : G^m \to G$ such that $\phi(a_1, \ldots, a_m) = \prod_{i=1}^m \phi_i(a_i)$. Note for $\phi \in \mathrm{Hom}_F(G^m, G)$, with restrictions ϕ_i to the factors, we have that $a \in \phi_i(G)$ and $b \in \phi_j(G)$ commute for $i \neq j$. Since $\phi_i(G)$ is 1 or G, if G is non-abelian we see that at most one ϕ_i can be non-trivial. Moreover, clearly the m-tuples $\mathrm{Hom}_F(G, G)^m$ where at most 1 coordinate is a non-trivial morphism in $\mathrm{Hom}_F(G, G)$ give elements of $\mathrm{Hom}_F(G^m, G)$. For an F-morphism $G \to G$, if it is non-trivial, it must be injective (since its kernel is a normal F-subgroup), and thus surjective. $\square$

8. Determination of $\mu_{u,n}$ on basic open sets

Recall that $X_{u,n}$ is the random group obtained by taking quotient of $\hat{F}_n$ by $n + u$ independent random relations from Haar measure. The goal of this section is to prove Theorem 8.1, in which we will give $\mathrm{Prob}((X_{u,n})^{\bar{S}} \simeq H)$ for every finite set S and finite level S group H, i.e. determine the measures of the basic open sets in the distributions coming from our random groups. Throughout this section, we assume $n \geq 1$, S is a finite set of finite groups, H is a finite level S group and

$$1 \to R \to F \to H \to 1$$

is the fundamental short exact sequence associated to S, n and H. For any abelian irreducible H-group G, we define $m(S, n, H, G)$ to be the multiplicity of G in R as an H-group under conjugation (see Lemma 5.11). Let G be a non-abelian finite group. Let G_i be the irreducible F-group structures one can put on G. Then we define $m(S, n, H, G)$ to be the sum (over i) of the multiplicity of the G_i in R as an F-group under conjugation. Equation (4.2) and Theorem 5.1 allow us to express $\mathrm{Prob}((X_{u,n})^{\bar{S}} \simeq H)$ in terms of the multiplicities $m(S, n, H, G)$. The work of this section will be to find explicit formulas for these $m(S, n, H, G)$ (given in Corollaries 8.8 and 8.10).

Theorem 8.1. *Let S be a finite set of finite groups and H a finite level S group. Let $n \geq 1$ and $u > -n$ be integers. Then*

(8.2) $\quad \mathrm{Prob}((X_{u,n})^{\bar{S}} \simeq H)$

$$= \frac{|\mathrm{Sur}(\hat{F}_n, H)|}{|\mathrm{Aut}(H)||H|^{n+u}} \prod_{G \in \mathcal{A}_H} \prod_{k=0}^{m(S,n,H,G)-1} (1 - \frac{h_H(G)^k}{|G|^{n+u}}) \prod_{G \in \mathcal{N}} (1 - |G|^{-n-u})^{m(S,n,H,G)},$$

and we have

(8.3)
$$\lim_{n\to\infty} \mathrm{Prob}((X_{u,n})^{\bar{S}} \simeq H)$$

$$= \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{G\in\mathcal{A}_H} \prod_{i=1}^{\infty} (1 - \lambda(S,H,G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G\in\mathcal{N}} e^{-|G|^{-u}\lambda(S,H,G)}.$$

Further, if $G \in \mathcal{A}_H \cup \mathcal{N}$ is isomorphic as a group to Γ^j for some simple group Γ, and either 1) Γ is not in the closure of S under taking subgroups and quotients, or 2) $j > |H|$, then $m(S,n,H,G) = \lambda(S,H,G) = 0$.

Remark 8.4. The products over $\mathcal{A}_H$ and $\mathcal{N}$ appearing in Theorem 8.1 are actually finite products (except for trivial terms), because of the last statement in the theorem.

Remark 8.5. We will show in Section 11 that statement of Theorem 8.1 also works for an arbitrary set S of finite groups.

First, we need to define the Möbius function on a poset of H-extensions. Given a finite group H, there is a poset $\mathcal{E}_H$ of H-extensions (*not* isomorphism classes of H-extensions) where $(E,\pi) \leq (E',\pi')$ if (E,π) is a sub-H-extension of (E',π'). (This relation is defined for literal sub-H-extensions and not H-extensions just isomorphic to a subextension.) We let $\nu(D,E)$ be the Möbius function of this poset (we drop the maps to H in the notation but they are implicit) so that for two H-extensions D and E we have

$$\nu(E,E) = 1$$

$$\nu(D,E) = - \sum_{\substack{D'\in\mathcal{E}_H \\ D<D'\leq E}} \nu(D',E) \qquad \text{if } D \neq E$$

so that in particular

$$\nu(D,E) = 0 \text{ if } D \text{ is not a sub-}H\text{-extension of } E$$

$$\sum_{\substack{D'\in\mathcal{E}_H \\ D\leq D'\leq E}} \nu(D',E) = \begin{cases} 1 & \text{if } D = E \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 7.1 relates our key multiplicities $m(S,n,H,G)$ to the number of F-surjections from R to G. An F-surjection $R \to G$ has a kernel K, and we have a surjection from our H-extension $(\hat{F}_n)^{\bar{S}} \to H$ to the H-extension $F/K \to H$. The next proposition will count such surjections of H-extensions.

Proposition 8.6. *Let $n \geq 1$ be an integer, S a finite set of finite groups, and H a finite level S group. Let $(\hat{F}_n)^{\bar{S}} \xrightarrow{\rho} H$ be an H-extension structure on $(\hat{F}_n)^{\bar{S}}$. Let $E \xrightarrow{\pi} H$ be a finite H extension. We have*

$$|\operatorname{Sur}(\rho,\pi)| = \begin{cases} \sum_{D\in\mathcal{E}_H, D\leq E} \nu(D,E) \left(\frac{|D|}{|H|}\right)^n & \text{if } E \text{ is level } S \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $(\hat{F}_n)^{\bar{S}} \to E$ is a surjection, then E is level S and hence $|\operatorname{Sur}(\rho,\pi)| = 0$ if E is not level S. If E is level S and $(D,\psi) \leq (E,\pi)$, surjections $(\hat{F}_n)^{\bar{S}} \to D$ exactly correspond to surjections $\hat{F}_n \to D$, i.e. choices of image for each generator $x_1, \ldots, x_n$ of $\hat{F}_n$ such that their

16

images generate D. For each generator x_i of $\hat{F}_n$, we have a fixed coset of $\ker(\pi)$ in D it can land in to actually obtain a surjection compatible with the maps to H. The number of homomorphisms $\hat{F}_n \to D$ where the generators go to the appropriate cosets is $(|D|/|H|)^n$. Let E' be a subgroup of D that could be generated by some $y_1, \ldots, y_n$ with each y_i in the required cosets of $\ker(\pi)$. Since ρ is a surjection, it follows that $\pi(E') = H$. So we have

$$\left(\frac{|D|}{|H|}\right)^n = \sum_{\substack{(E',\phi)\in\mathcal{E}_H \\ (E',\phi)\leq(D,\psi)}} |\operatorname{Sur}_H(\rho,\phi)|.$$

Using Möbius inversion, we obtain the result. We can sum the above as follows. Given a finite H-extension (E,π) of level S, we have

$$\sum_{(D,\psi)\leq(E,\pi)} \nu(D,E)\left(\frac{|D|}{|H|}\right)^n = \sum_{(D,\psi)\leq(E,\pi)} \nu(D,E) \sum_{(E',\phi)\leq(D,\psi)} |\operatorname{Sur}_H(\rho,\phi)|$$

$$= \sum_{(E',\phi)\leq(E,\pi)} |\operatorname{Sur}_H(\rho,\phi)| \sum_{(E',\phi)\leq(D,\psi)\leq(E,\pi)} \nu(D,E)$$

$$= |\operatorname{Sur}_H(\rho,\pi)|,$$

as desired. $\qquad\square$

Now we will build on Proposition 8.6 to find $|\operatorname{Sur}_F(R,G)|$, after which we can then use Theorem 7.1 to find the $m(S,n,H,G)$. We will first do the case of abelian G, and then non-abelian G.

Proposition 8.7 (Counting surjections from R to abelian G). *Let H, F, and R be defined as at the beginning of this section. Let G be an abelian irreducible F-group. Then*

$$|\operatorname{Sur}_F(R,G)| = |\operatorname{Aut}_F(G)| \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker\pi \simeq G \text{ as an } H\text{-group} \\ E \text{ is level } S}} \frac{\sum_{D\in\mathcal{E}_H, D\leq E} \nu(D,E)\left(\frac{|D|}{|H|}\right)^n}{|\operatorname{Aut}_H(E,\pi)|}.$$

if the action of F on G factors through $F \to H$ (i.e. elements of R act trivially on G) and $|\operatorname{Sur}_F(R,G)| = 0$ otherwise.

Proof. We have that $|\operatorname{Sur}_F(R,G)|$ is $|\operatorname{Aut}_F(G)|$ times the number of F-subgroups M of R such that R/M under F-conjugation is isomorphic to G as an F-group. If M is an F-subgroup of R such that R/M is abelian, then the action of F via conjugation on R/M factors through H (because conjugation by elements from R is trivial in R/M as R/M is abelian). So suppose that the action of F on G factors through H. We have the number of F-subgroups M of R such that R/M is isomorphic to G as an F-group is

$$\sum_{\substack{\text{isom. classes of} \\ H\text{-extensions } (E,\pi)}} \#\left\{ F\text{-subgroups } M \text{ of } R \,\middle|\, \begin{matrix} (F/M \to H) \simeq (E,\pi) \text{ as } H\text{-exts,} \\ R/M \simeq G \text{ as } F\text{-groups} \end{matrix} \right\}$$

$$= \sum_{\substack{\text{isom. classes of} \\ H\text{-extensions } (E,\pi) \\ \ker\pi\simeq G \text{ as groups}}} \#\left\{ F\text{-subgroups } M \text{ of } R \,\middle|\, \begin{matrix} (F/M \to H) \simeq (E,\pi) \text{ as } H\text{-exts,} \\ R/M \simeq G \text{ as } F\text{-groups} \end{matrix} \right\}.$$

17

Given that R/M is abelian (which is guaranteed by the group isomorphism $\ker \pi \simeq G$ and the H-extension isomorphism $(F/M \to H) \simeq (E, \pi)$), since the action of F on R/M factors through H, we have that R/M is isomorphic to G as an F-group if and only if it is isomorphic to G as an H-group. Given $(F/M \to H) \simeq (E, \pi)$, this is the same as requiring $\ker \pi \simeq G$ as an H-group. Thus the above sum is equal to

$$\sum_{\substack{\text{isom. classes of } H\text{-extension } (E,\pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group}}} \#\left\{F\text{-subgroups } M \text{ of } R \mid (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts}\right\}$$

$$= \sum_{\substack{\text{isom. classes of } H\text{-extension } (E,\pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group}}} \frac{\#\left\{(M, \phi) \,\middle|\, \begin{array}{l} M \text{ an } F\text{-subgroup of } R \\ \phi : (F/M \to H) \simeq (E, \pi) \end{array}\right\}}{|\operatorname{Aut}_H(E, \pi)|}.$$

Note that the data (M, ϕ) above is exactly the same as the data of a surjection of H-extensions from $F \to H$ to $E \to H$.

Now let (E, π) be an H-extension with $\ker \pi$ (via conjugation) an abelian irreducible H-group. Consider a surjection of H-extensions from $(\hat{F}_n)^{\bar{S}} \to H$ to $E \to H$, in which the map $(\hat{F}_n)^{\bar{S}} \to E$ has kernel K. Let N denote the kernel of $(\hat{F}_n)^{\bar{S}} \to H$. Then $N/K \simeq \ker \pi$ is an irreducible $(\hat{F}_n)^{\bar{S}}$-group, and so K is a maximal proper $(\hat{F}_n)^{\bar{S}}$-subgroup of N. So the map $(\hat{F}_n)^{\bar{S}} \to E$ factors through F. On the other hand, any surjection of H-extensions from $F \to H$ to $E \to H$ clearly extends to a surjection of H-extensions from $(\hat{F}_n)^{\bar{S}} \to H$ to $E \to H$. Thus the above sum is equal to

$$\sum_{\substack{\text{isom. classes of } H\text{-extensions } (E, \pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group}}} \frac{|\operatorname{Sur}_H((\hat{F}_n)^{\bar{S}} \to H, \pi)|}{|\operatorname{Aut}_H(E, \pi)|}.$$

The result now follows from applying Proposition 8.6 above, after dividing out by the number of choices of isomorphism to (E, π). $\qquad\square$

We now can determine the multiplicities of the abelian irreducible F-groups in R by combining Theorem 7.1 and Proposition 8.7.

Corollary 8.8 (Multiplicities of abelian G in R). *Let H, F and R be as above. Let G be an abelian irreducible H-group. Then*

$$\frac{h_H(G)^{m(S,n,H,G)} - 1}{h_H(G) - 1} = \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group} \\ E \text{ is level } S}} \frac{\sum_{D \in \mathcal{E}_H, D \leq E} \nu(D, E) \left(\frac{|D|}{|H|}\right)^n}{|\operatorname{Aut}_H(E, \pi)|}.$$

Next, we will apply a similar plan to obtain the multiplicities of the non-abelian G, but there is an important difference from the abelian case. When $\ker(E \xrightarrow{\pi} H)$ is non-abelian, a surjection of H-extensions $F \to E$ still gives an F-group structure on $\ker \pi$ by conjugation in E, but, unlike in the case when $\ker \pi$ is abelian, that F-group structure is not necessarily determined by the isomorphism type of the H-extension (E, π). So in this case it is most

convenient to add together, for each possible *underlying group* G of a non-abelian irreducible F-group, all surjections $F \to E$ over all G extensions E of H.

Proposition 8.9 (Counting surjections from R to non-abelian G). *Let H, F and R be as above. Let G be a finite non-abelian group. Let G_i be the pairwise non-isomorphic irreducible F-group structures on G for $1 \le i \le k$ (k may be 0). Then*

$$\sum_{i=1}^{k} \frac{|\operatorname{Sur}_F(R, G_i)|}{|\operatorname{Aut}_F(G_i)|} = \sum_{\substack{isom.\ classes\ of\ H\text{-}extensions\ (E, \pi) \\ \ker \pi \simeq G \\ \ker \pi\ irred.\ E\text{-}group \\ E\ is\ level\ S}} \frac{\sum_{D \in \mathcal{E}_H, D \le E} \nu(D, E) \left(\frac{|D|}{|H|}\right)^n}{|\operatorname{Aut}_H(E, \pi)|}.$$

Proof. We note that $|\operatorname{Sur}_F(R, G_i)|/|\operatorname{Aut}_F(G_i)|$ is the number of F-subgroups of R whose corresponding quotient is isomorphic to G_i as an F-group. We have

$$\sum_{i=1}^{k} \frac{|\operatorname{Sur}_F(R, G_i)|}{|\operatorname{Aut}_F(G_i)|}$$

$$= \sum_{i=1}^{k} \sum_{\substack{isom.\ classes\ of \\ H\text{-}extensions\ (E, \pi)}} \# \left\{ F\text{-subgroups } M \text{ of } R \;\middle|\; \begin{array}{l} (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts} \\ R/M \simeq G_i \text{ as } F\text{-groups} \end{array} \right\}$$

$$= \sum_{i=1}^{k} \sum_{\substack{isom.\ classes\ of \\ H\text{-}extensions\ (E, \pi) \\ \ker \pi \simeq G}} \# \left\{ F\text{-subgroups } M \text{ of } R \;\middle|\; \begin{array}{l} (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts} \\ R/M \simeq G_i \text{ as } F\text{-groups} \end{array} \right\}$$

$$= \sum_{\substack{isom.\ classes\ of \\ H\text{-}extensions\ (E, \pi) \\ \ker \pi \simeq G}} \sum_{i=1}^{k} \# \left\{ F\text{-subgroups } M \text{ of } R \;\middle|\; \begin{array}{l} (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts} \\ R/M \simeq G_i \text{ as } F\text{-groups} \end{array} \right\}$$

$$= \sum_{\substack{isom.\ classes\ of \\ H\text{-}extensions\ (E, \pi) \\ \ker \pi \simeq G \\ \ker \pi\ irred.\ E\text{-}group}} \sum_{i=1}^{k} \# \left\{ F\text{-subgroups } M \text{ of } R \;\middle|\; \begin{array}{l} (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts} \\ R/M \simeq G_i \text{ as } F\text{-groups} \end{array} \right\}$$

$$= \sum_{\substack{isom.\ classes\ of\ H\text{-}extensions\ (E, \pi) \\ \ker \pi \simeq G \\ \ker \pi\ irred.\ E\text{-}group}} \# \{ F\text{-subgroups } M \text{ of } R \,|\, (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts} \}$$

$$= \sum_{\substack{isom.\ classes\ of\ H\text{-}extensions\ (E, \pi) \\ \ker \pi \simeq G \\ \ker \pi\ irred.\ E\text{-}group}} \frac{\# \left\{ (M, \phi) \;\middle|\; \begin{array}{l} M \text{ an } F\text{-subgroup of } R \\ \phi : (F/M \to H) \simeq (E, \pi) \text{ as } H\text{-exts} \end{array} \right\}}{|\operatorname{Aut}_H(E, \pi)|}.$$

The second equality follows because $(F/M \to H) \simeq (E, \pi)$ and $R/M \simeq G_i$ imply that $\ker \pi \simeq G$. The fourth equality follows because $(F/M \to H) \simeq (E, \pi)$ and R/M being an irreducible F-group imply that $\ker \pi$ is an irreducible E-group. The fifth equality follows

19

because $\ker \pi \simeq G$ and $\ker \pi$ being an irreducible E-group and $(F/M \to H) \simeq (E, \pi)$ imply that R/M is isomorphic to some G_i as an F-group.

Then we obtain the desired result by applying the same argument as at the end of Proposition 8.7. $\qquad\square$

We now can determine the multiplicities of the non-abelian irreducible F-groups in R by combining Theorem 7.1 and Proposition 8.9.

Corollary 8.10 (Multiplicities of non-abelian G in R). *Let H, F and R be as above. Let G be an non-abelian finite group. Then*

$$m(S, n, H, G) = \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker \pi \simeq G \\ \ker \pi \text{ irred. } E\text{-group} \\ E \text{ level } S}} \frac{\sum_{D \in \mathcal{E}_H, D \leq E} \nu(D, E) \left(\frac{|D|}{|H|}\right)^n}{|\operatorname{Aut}_H(E, \pi)|}.$$

Finally, before we prove Theorem 8.1, we need the following lemma, whose proof is straightforward.

Lemma 8.11. *Suppose $x_1, x_2, \ldots$ is a sequence of real numbers with limit x, and $y_1, \ldots$ is a sequence of real numbers with limit ∞. Let $a > 1$ be a real number. Then $f(x) = \prod_{i=1}^{\infty}(1 - xa^{-i})$ is continuous in x and*

$$\lim_{n \to \infty} \prod_{i=1}^{y_n}(1 - x_n a^{-i}) = \prod_{i=1}^{\infty}(1 - xa^{-i}).$$

Proof of Theorem 8.1. Equation (4.2) and Theorem 5.1 establish Equation (8.2) of Theorem 8.1. Recall that for G a finite abelian irreducible H-group, we have defined

$$\lambda(S, H, G) := (h_H(G) - 1) \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \text{such that } \ker \pi \simeq G \text{ as } H\text{-groups,} \\ \text{and } E \text{ is level } S}} \frac{1}{|\operatorname{Aut}_H(E, \pi)|}$$

and Corollary 8.8 gives that

$$\frac{h_H(G)^{m(S,n,H,G)} - 1}{h_H(G) - 1} = \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group} \\ E \text{ is level } S}} \frac{\sum_{D \in \mathcal{E}_H, D \leq E} \nu(D, E) \left(\frac{|D|}{|H|}\right)^n}{|\operatorname{Aut}_H(E, \pi)|}.$$

So we have

$$\lim_{n \to \infty} \frac{h_H(G)^{m(S,n,H,G)}}{|G|^n} = \lim_{n \to \infty} \frac{h_H(G)^{m(S,n,H,G)} - 1}{|G|^n}$$

$$= \lim_{n \to \infty} \frac{h_H(G) - 1}{|G|^n} \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group} \\ E \text{ is level } S}} \frac{\sum_{D \in \mathcal{E}_H, D \leq E} \nu(D, E) \left(\frac{|D|}{|H|}\right)^n}{|\operatorname{Aut}_H(E, \pi)|}.$$

Note for any $D \neq E$ in the above sum, we have $\lim_{n \to \infty} |D|^n |H|^{-n} |G|^{-n} = 0$. Thus we conclude (and similarly in the non-abelian case using Corollary 8.10) that $\lambda(S, H, G)$ is

related to $m(S, n, H, G)$ as follows:

$$(8.12) \qquad \lim_{n \to \infty} \frac{h_H(G)^{m(S,n,H,G)}}{|G|^n} = \lambda(S, H, G) \qquad\qquad \text{for } G \in \mathcal{A}_H$$

$$\lim_{n \to \infty} \frac{m(S, n, H, G)}{|G|^n} = \lambda(S, H, G) \qquad\qquad \text{for } G \in \mathcal{N}.$$

Remark 8.13. Note that since by Remark 5.2, for $G \in \mathcal{A}_H$, we have that $|G|$ is a power of $h_H(G)$, it follows that $\lambda(S, H, G)$ is an integral power of $h_H(G)$, and that the limit above stabilizes for sufficiently large n.

We next establish the final statement of Theorem 8.1. Since any irreducible F-group factor of R is in $\bar{S}$, Corollary 6.12 shows that it is a power of a simple group in the closure of S under taking subgroups and quotients. Lemma 6.1 shows that the power is bounded by $|H|$, showing the final statement of Theorem 8.1.

To establish Equation (8.3), it will suffice to take the limit of a factor in Equation (8.2) corresponding to a single G (since there are only finitely many G with non-trivial factors, independent of n, by Lemma 6.10 and Corollary 6.13). The factor in Equation (8.2) for a $G \in \mathcal{A}_H$ is

$$\prod_{k=0}^{m(S,n,H,G)-1} (1 - \frac{h_H(G)^k}{|G|^{n+u}}) = \prod_{i=1}^{m(S,n,H,G)} (1 - \frac{h_H(G)^{m(S,n,H,G)} h_H(G)^{-i}}{|G|^{n+u}}).$$

If there are no extensions E in the sum in Corollary 8.8, then $m(S, n, H, G)$ and $\lambda(S, H, G)$ are 0. Otherwise $\lambda(S, H, G) > 0$, and thus it follows from Equation (8.12) that $m(S, n, H, G) \to \infty$ as $n \to \infty$. So using Lemma 8.11 and Equation (8.12), we obtain the limit in Equation (8.3) for a single factor $G \in \mathcal{A}_H$. In a similar but simpler fashion, from Equation (8.12), we obtain the limit in Equation (8.3) for a single factor $G \in \mathcal{N}$. This completes the proof of Theorem 8.1. $\qquad\qquad \square$

9. COUNTABLE ADDITIVITY OF μ_u

The goal of this section is to prove Theorem 9.1 which states that μ_u defined in Equation (3.1) is countably additive on the algebra $\mathcal{A}$. It then follows from Carathéodory's extension theorem that μ_u can be uniquely extended to a measure on the Borel sets of $\mathcal{P}$. The heart the proof of Theorem 9.1 is Theorem 9.2. We will first prove Theorem 9.2 in Section 9.1, and then prove Theorem 9.1 in Section 9.2.

Theorem 9.1. *Let u be an integer. Then μ_u is countably additive on the algebra $\mathcal{A}$ generated by the $U_{S,H}$ for S a finite set of finite groups and H a finite group.*

Theorem 9.2. *Let ℓ be a positive integer. Recall that S_ℓ is defined to be the set consisting of all groups of order less than or equal to ℓ. For a non-negative integer u, we have*

$$\sum_{H \text{ is finite and level } \ell} \mu_u(U_{S_\ell,H}) = 1.$$

9.1. Proof of Theorem 9.2. Assume ℓ is a positive integer, H is a finite level ℓ group and let $\tilde{H} = H^{\bar{S}_{\ell-1}}$. In Lemmas 9.3 and 9.4, we will first give upper bounds for the number of irreducible factors G with non-zero $m(S_\ell, n, H, G)$ for some n that are isomorphic to a given underlying group M.

Lemma 9.3. *Suppose M is a direct product of isomorphic abelian simple groups. Then*

$$\# \left\{ G \in \mathcal{A}_H \,\middle|\, \begin{array}{l} G \simeq M \text{ and} \\ m(S_\ell, n, H, G) \neq 0 \text{ for some } n \end{array} \right\} \leq \sum_{(M,A) \in \mathcal{CF}(\bar{S}_\ell)} |\operatorname{Sur}(\tilde{H}, A)|,$$

where the notation on the right-hand side above means that the sum is taken over all chief factor pairs in $\mathcal{CF}(\bar{S}_\ell)$ whose first components are isomorphic to M as groups.

Proof. We give an injection

$$\left\{ G \in \mathcal{A}_{H}, \phi \,\middle|\, \begin{array}{l} \phi : G \simeq M \text{ and} \\ m(S_\ell, n, H, G) \neq 0 \text{ for some } n \end{array} \right\} \to \{(M, A) \in \mathcal{CF}(\bar{S}_\ell), \pi \,|\, \pi \in \operatorname{Sur}(H, A)\}.$$

Consider $G \in \mathcal{A}_H$ and $\phi : G \simeq M$ such that $m(S_\ell, n, H, G) \neq 0$ for some n. Assume

$$1 \to R \to F \to H \to 1$$

is the fundamental short exact sequence associated to S_ℓ, n, and H. Then G appears as a factor in R and $(G, \rho_G(F)) \in \mathcal{CF}(\bar{S}_\ell)$. Using $\phi : G \simeq M$, we have that the quotient $\rho_G(F)$ of H acts on M, and so $(M, \rho_G(F)) \in \mathcal{CF}(\bar{S}_\ell)$. We let π be the quotient map from H to $\rho_G(F)$. Given $(M, A) \in \mathcal{CF}(\bar{S}_\ell)$ and $\pi \in \operatorname{Sur}(H, A)$, we can use π to give M the structure of an irreducible H-group, and let ϕ be the identity. This recovers G and ϕ, though possibly without $m(S_\ell, n, H, G) \neq 0$. By Corollary 6.13, if $(M, A) \in \mathcal{CF}(\bar{S}_\ell)$, then $A/\operatorname{Inn}(M) \simeq A$ is a group of level $\ell - 1$. Then by the definition of pro-$\bar{S}$ completion, $\operatorname{Sur}(H, A)$ is one-to-one corresponding to $\operatorname{Sur}(\tilde{H}, A)$ and we finish the proof. $\qquad\square$

Similarly, for non-abelian irreducible factors, we have the following lemma.

Lemma 9.4. *Suppose M is a direct product of isomorphic non-abelian simple groups. Then*

$$\# \left\{ \text{isom. classes of H-extensions } (E, \pi) \,\middle|\, \begin{array}{l} \ker \pi \simeq M \text{ is irred. E-group} \\ E \text{ is level } \ell \end{array} \right\}$$

$$\leq \sum_{(M,A) \in \mathcal{CF}(\bar{S}_\ell)} |\operatorname{Sur}(\tilde{H}, A/\operatorname{Inn}(M))|.$$

Proof. We give an injection

$$\left\{ \text{isom. classes of H-extensions } (E, \pi) \,\middle|\, \begin{array}{l} \ker \pi \simeq M \text{ is irred. E-group} \\ E \text{ is level } \ell \end{array} \right\}$$

$$\to \quad \{(M, A) \in \mathcal{CF}(\bar{S}_\ell), \phi \,|\, \phi \in \operatorname{Sur}(H, A/\operatorname{Inn}(M))\}.$$

Consider an isomorphism class of H-extension (E, π) such that $\ker \pi \simeq M$ is an irreducible E-group and E is level ℓ. Then $(\ker \pi, \rho_{\ker \pi}(E)) \in \mathcal{CF}(\bar{S}_\ell)$, and $\rho_{\ker \pi}$ induces a surjection $\phi : H \to \rho_{\ker \pi}(E)/\operatorname{Inn}(M)$ since $\rho_{\ker \pi}$ is an isomorphism when restricted on $\ker \pi$ that maps $\ker \pi$ to $\operatorname{Inn}(M)$. Suppose $(M, A) \in \mathcal{CF}(\bar{S}_\ell)$ and $\phi \in \operatorname{Sur}(H, A/\operatorname{Inn}(M))$. If two H-extensions (E_1, π_1) and (E_2, π_2) both map to (M, A) and ϕ, then from the diagram below

we see that E_1 and E_2 are both the fiber product of ϕ and $A \to A/\operatorname{Inn}(M)$, so (E_1, π_1) and (E_2, π_2) are isomorphic as H-extensions. Therefore, the map defined at the begin of the proof is an injection. Then the lemma follows as $\operatorname{Sur}(H, A)$ is one-to-one corresponding to $\operatorname{Sur}(\widetilde{H}, A)$.

Let $P_{u,n}(U_{S_\ell, H})$ denote the product in Equation (8.2), i.e.

$$P_{u,n}(U_{S_\ell,H}) = \prod_{G \in \mathcal{A}_H} \prod_{k=0}^{m(S_\ell, n, H, G)-1} \left(1 - \frac{h_H(G)^k}{|G|^{n+u}}\right) \prod_{G \in \mathcal{N}} (1 - |G|^{-n-u})^{m(S_\ell, n, H, G)}.$$

Lemma 9.5. *Suppose $\ell > 1$, $n \geq 1$ and $u > -n$ are integers and $\widetilde{H}$ is a finite level $\ell - 1$ group. Then there exists a non-zero constant $c(u, \ell, \widetilde{H})$ depending on u, ℓ and $\widetilde{H}$ such that, for every finite level ℓ group H with $H^{\bar{S}_{\ell-1}} = \widetilde{H}$, either $P_{u,n}(U_{S_\ell,H}) \geq c(u, \ell, \widetilde{H})$ or $P_{u,n}(U_{S_\ell,H}) = 0$.*

Proof. For each $G \in \mathcal{A}_H$, G is a direct product of isomorphic abelian simple groups, i.e. G is a direct product of $\mathbb{Z}/p\mathbb{Z}$ for some prime p. By Remark 5.2, $h_H(G)$ is a power of p and $|G|$ is a power of $h_H(G)$. Note that both of the trivial map (every element maps to 1) and the identity map of G respect the H-action, therefore $h_H(G) > 1$. So if the product $\prod_{k=0}^{m(S_\ell, n, H, G)-1}(1 - \frac{h_H(G)^k}{|G|^{n+u}})$ is nonzero, then it is a product of $1 - p^{-i}$ for distinct positive integers i, which is greater than $\prod_{k=1}^{\infty}(1 - p^{-k}) \geq \prod_{k=1}^{\infty}(1 - 2^{-k})$. If $P_{u,n}(U_{S_\ell,H}) \neq 0$, then

$$\prod_{G \in \mathcal{A}_H} \prod_{k=0}^{m(S_\ell, n, H, G)-1} \left(1 - \frac{h_H(G)^k}{|G|^{n+u}}\right) = \prod_{\substack{G \in \mathcal{A}_H \text{ and} \\ m(S_\ell, n, H, G) \neq 0}} \prod_{k=0}^{m(S_\ell, n, H, G)-1} \left(1 - \frac{h_H(G)^k}{|G|^{n+u}}\right)$$

$$\geq \prod_{\substack{G \in \mathcal{A}_H \text{ and} \\ m(S_\ell, n, H, G) \neq 0 \text{ for some } n}} \prod_{k=1}^{\infty}(1 - 2^{-k})$$

$$= \left[\prod_{k=1}^{\infty}(1 - 2^{-k})\right]^{\#\{G \in \mathcal{A}_H \,|\, m(S_\ell, n, H, G) \neq 0 \text{ for some } n\}}$$

$$\geq \left[\prod_{k=1}^{\infty}(1 - 2^{-k})\right]^{\sum_{\substack{(M,A) \in \mathcal{CF}(\bar{S}_\ell) \\ M \text{ is abelian}}} |\operatorname{Sur}(\widetilde{H}, A)|},$$

where the last inequality follows from Lemma 9.3. Therefore, if $P_{u,n}(U_{S_\ell,H})$ is non-zero, then its abelian part has a lower bound depending only on ℓ and $\widetilde{H}$. Similarly, for the non-abelian part, we consider

$$\prod_{G \in \mathcal{N}} (1 - |G|^{-n-u})^{m(S_\ell,n,H,G)} \geq \prod_{G \in \mathcal{N}} \left[\left(1 - \frac{1}{2}\right)^2 \right]^{\frac{m(S_\ell,n,H,G)}{|G|^{n+u}}}$$

$$= \left[\left(1 - \frac{1}{2}\right)^2 \right]^{\sum_{G \in \mathcal{N}} \frac{m(S_\ell,n,H,G)}{|G|^{n+u}}},$$

where the first inequality follows because $(1 - \frac{1}{n})^n$ is an increasing sequence. Then we have

$$\sum_{G \in \mathcal{N}} \frac{m(S_\ell, n, H, G)}{|G|^{n+u}}$$

$$= \sum_{G \in \mathcal{N}} |G|^{-u} \left(\sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker \pi \simeq G \\ \ker \pi \text{ irred. } E\text{-group} \\ E \text{ is level } \ell}} \frac{|G|^{-n} \sum_{D \in \mathcal{E}_H, D \leq E} \nu(D,E) \frac{|D|^n}{|H|}}{|\operatorname{Aut}_H(E,\pi)|} \right)$$

$$\leq \sum_{G \in \mathcal{N}} |G|^{-u} \# \left\{ \text{isom. classes of } H\text{-extensions } (E,\pi) \, \middle| \, \begin{array}{l} \ker \pi \simeq G \text{ is irred. } E\text{-group} \\ E \text{ is level } \ell \end{array} \right\}$$

$$\leq \sum_{G \in \mathcal{N}} |G|^{-u} \left(\sum_{(G,A) \in \mathcal{CF}(\bar{S}_\ell)} |\operatorname{Sur}(\widetilde{H}, A/\operatorname{Inn}(G))| \right)$$

$$= \sum_{\substack{(G,A) \in \mathcal{CF}(\bar{S}_\ell) \\ G \text{ non-abelian}}} |G|^{-u} |\operatorname{Sur}(\widetilde{H}, A/\operatorname{Inn}(G))|.$$

The first equality above is Corollary 8.10. The first inequality follows from the fact that $|\operatorname{Sur}(\rho, \pi)|$ in Proposition 8.6 is less than or equal to $|G|^n$. The second inequality follows by Lemma 9.4. It shows that the non-abelian part also has a lower bound depending on u, ℓ and $\widetilde{H}$. By Corollary 6.13, $\mathcal{CF}(\bar{S}_\ell)$ is a finite set, so these lower bounds for abelian part and non-abelian parts are both non-zero. Then we proved the theorem. $\qquad \square$

Now, we establish the inductive step that is crucial in the proof of Theorem 9.2.

Lemma 9.6. *Let $\ell > 1$, $n \geq 1$, $u > -n$ be integers, and $\widetilde{H}$ be a finite level $\ell - 1$ group. Then*

$$\lim_{n \to \infty} \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H} = H^{\bar{S}_{\ell-1}}}} \mu_{u,n}(U_{S_\ell,H}) = \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H} = H^{\bar{S}_{\ell-1}}}} \mu_u(U_{S_\ell,H}).$$

Proof. Assume H is finite and level ℓ such that $\widetilde{H} = H^{\bar{S}_{\ell-1}}$. Let $i(H)$ be the smallest integer such that $|\operatorname{Sur}(\hat{F}_n, H)|/|H|^n \geq \frac{1}{2}$ for all $n > i(H)$ (note that $i(H)$ is finite since

24

$\lim_{n\to\infty} |\operatorname{Sur}(\hat{F}_n, H)|/|H|^n = 1)$. Then either $\mu_{u,n}(U_{S_\ell,H}) = 0$ or

$$\mu_{u,n}(U_{S_\ell,H}) = \frac{|\operatorname{Sur}(\hat{F}_n, H)|}{|\operatorname{Aut}(H)||H|^{n+u}} P_{u,n}(U_{S_\ell,H})$$

$$\geq \frac{1}{2} c(u, \ell, \widetilde{H}) \frac{1}{|\operatorname{Aut}(H)||H|^u}$$

for $n > i(H)$, by Lemma 9.5. We call H *achievable* if it is finite level ℓ and there exists n such that $\mu_{u,n}(U_{S_\ell,H}) \neq 0$ (we will give an equivalent definition in Section 13). The function $\mu_{u,n}(U_{S_\ell,H})$ of H is dominated by the function of H that is $\frac{1}{|\operatorname{Aut}(H)||H|^u}$ when H is achievable and 0 otherwise. We will next show that the sum of this dominating function converges, in order to use Lebesgue's Dominated Convergence Theorem. We have

$$\sum_{\substack{H \text{ is achievable} \\ \text{s.t. } \widetilde{H} \simeq H^{\bar{S}_{\ell-1}}}} \frac{1}{|\operatorname{Aut}(H)||H|^u} = \lim_{n\to\infty} \sum_{\substack{H \text{ is achievable} \\ \text{s.t. } \widetilde{H} \simeq H^{\bar{S}_{\ell-1}} \\ \text{and } i(H)<n}} \frac{1}{|\operatorname{Aut}(H)||H|^u}$$

$$\leq \lim_{n\to\infty} \frac{2}{c(u, \ell, \widetilde{H})} \sum_{\substack{H \text{ is achievable} \\ \text{s.t. } \widetilde{H} \simeq H^{\bar{S}_{\ell-1}} \\ \text{and } i(H)<n}} \mu_{u,n}(U_{S_\ell,H})$$

$$\leq \frac{2}{c(u, \ell, \widetilde{H})},$$

where the first equality expresses the implicit infinite sum as an explicit limit. Thus by Lebesgue's Dominated Convergence Theorem,

$$\lim_{n\to\infty} \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H} \simeq H^{\bar{S}_{\ell-1}}}} \mu_{u,n}(U_{S_\ell,H}) = \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H} \simeq H^{\bar{S}_{\ell-1}}}} \lim_{n\to\infty} \mu_{u,n}(U_{S_\ell,H}),$$

which completes the lemma. $\qquad\square$

Proof of Theorem 9.2. We proceed by induction on ℓ. When $\ell = 1$, note that the trivial group is the only group that is finite level 1 and it's obvious that $\mu_u(U_{S_1,1}) = 1$. Assume the theorem is true for $\ell - 1$, i.e.

$$\sum_{\widetilde{H} \text{ is finite level } \ell-1} \mu_u(U_{S_{\ell-1},\widetilde{H}}) = 1.$$

We see that for any finite level $\ell - 1$ group $\widetilde{H}$

$$\mu_u(U_{S_{\ell-1},\widetilde{H}}) = \lim_{n\to\infty} \mu_{u,n}(U_{S_{\ell-1},\widetilde{H}})$$

$$= \lim_{n\to\infty} \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H} = H^{\bar{S}_{\ell-1}}}} \mu_{u,n}(U_{S_\ell,H})$$

$$= \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H} = H^{\bar{S}_{\ell-1}}}} \mu_u(U_{S_\ell,H}),$$

25

where the second equality above follows from the definition of $\mu_{u,n}$ on basic open sets and the last step follows from Lemma 9.6. Therefore, we finish the proof by

$$
\begin{aligned}
\sum_{H \text{ is finite level } \ell} \mu_u(U_{S_\ell,H}) &= \sum_{\substack{\widetilde{H} \text{ is finite level } \ell-1}} \sum_{\substack{H \text{ is finite level } \ell \\ \text{s.t. } \widetilde{H}=H^{\bar{S}_{\ell-1}}}} \mu_u(U_{S_\ell,H}) \\
&= \sum_{\widetilde{H} \text{ is finite level } \ell-1} \mu_u(U_{S_{\ell-1},\widetilde{H}}) \\
&= 1.
\end{aligned}
$$

$\square$

9.2. **Proof of Theorem 9.1.** We will use the following corollary of Theorem 9.2.

Corollary 9.7. *Let ℓ be a positive integer, and $B = \cup_{j=1}^\infty U_{S_\ell,H_j}$ for some finite groups H_j such that $U_{S_\ell,H_j} \neq U_{S_\ell,H_{j'}}$ for $j \neq j'$ (note that $U_{S_\ell,H_j} \neq U_{S_\ell,H_{j'}}$ implies $U_{S_\ell,H_j} \cap U_{S_\ell,H_{j'}} = \emptyset$). Suppose that $B \in \mathcal{A}$, the algebra of sets generated by the basic open sets $U_{S,G}$ for a finite set S of finite groups and a finite level S group G. Let u be an integer. Then $\mu_u(B) = \sum_{j=1}^\infty \mu_u(U_{S_\ell,H_j})$.*

Proof. Since μ_u is defined as a limit of measures $\mu_{u,n}$, it is immediate that μ_u is finitely additive because finite sums can be exchanged with the limit. Let G_j be the level ℓ finite groups not among the H_j. Then for every positive integer M, we have

$$
\sum_{j=1}^M \mu_u(U_{S_\ell,H_j}) \leq \mu_u(B) \leq 1 - \sum_{j=1}^M \mu_u(U_{S_\ell,G_j}).
$$

Taking limits as $M \to \infty$ gives

$$
\sum_{j=1}^\infty \mu_u(U_{S_\ell,H_j}) \leq \mu_u(B) \leq 1 - \sum_{j=1}^\infty \mu_u(U_{S_\ell,G_j}) = \sum_{j=1}^\infty \mu_u(U_{S_\ell,H_j}),
$$

where the last equality is by Theorem 9.2. $\square$

Proof of Theorem 9.1. If we have disjoint sets $A_n \in \mathcal{A}$ with $A = \cup_{n\geq 1} A_n \in \mathcal{A}$, by taking $B_n = A \setminus \cup_{j=1}^n A_j$, it suffices to show that for $B_1 \supset B_2 \supset \ldots$ (with $B_n \in \mathcal{A}$) with $\cap_{n\geq 1} B_n = \emptyset$ we have $\lim_{n\to\infty} \mu_u(B_n) = 0$.

We can assume, without loss of generality, that for each $\ell \geq 1$, we have $B_\ell = \cup_j U_{S_\ell,G_{\ell,j}}$ (i.e. B_ℓ is defined at level ℓ). (Note that when all groups in S have order at most m that $U_{S,H}$ is a union of sets of the form $U_{S_m,G}$ for varying G. We can always insert redundant B_i's if the level required to define the B_ℓ increase quickly.) We will show by contradiction that $\lim_{\ell\to\infty} \mu_u(B_\ell) = 0$.

Suppose, instead that there is an $\epsilon > 0$ such that for all ℓ, we have $\mu_u(B_\ell) \geq \epsilon$. It follows from Corollary 9.7 that for each ℓ we have a subset $K_\ell \subset B_\ell$ such that $\mu_u(B_\ell \setminus K_\ell) < \epsilon/2^{\ell+1}$ and K_ℓ is a *finite* union of $U_{S_\ell,G_{\ell,j}}$.

Next, let $C_\ell = \cap_{j=1}^\ell K_j$. Then $\mu_u(B_\ell \setminus C_\ell) < \epsilon/2$, since

$$
\begin{aligned}
\mu_u(B_\ell \setminus C_\ell) =& \mu_u(B_\ell \setminus K_\ell) + \mu_u(K_\ell \setminus K_\ell \cap K_{\ell-1}) + \cdots + \mu_u(K_\ell \cap \cdots \cap K_2 \setminus K_\ell \cap \cdots \cap K_1) \\
<& \epsilon/2^{\ell+1} + \mu_u(B_{\ell-1} \setminus K_{\ell-1}) + \cdots + \mu_u(B_1 \setminus K_1)
\end{aligned}
$$

$$< \epsilon/2^{\ell+1} + \epsilon/2^\ell + \cdots + \epsilon/2^2.$$

So $\mu_u(C_\ell) \geq \epsilon/2$ for each ℓ and in particular it is non-empty. Note $C_{\ell+1} \subset C_\ell$ for all ℓ. Pick $x_\ell \in C_\ell$ for all ℓ.

Note C_ℓ is defined at level ℓ and a finite union of the basic open sets $U_{S_\ell, G_{\ell,j}}$. Pick an H_1 so that infinitely many of the x_ℓ are in U_{S_1, H_1} (this is possible since all x_ℓ are in C_1 and there are only finitely many $U_{S_1, H}$ that make up C_1), and then disregard the x_ℓ that are not in U_{S_1, H_1}. In particular note $U_{S_1, H_1} \subset C_1$. Then pick H_2 so that infinitely many of the remaining x_ℓ are in U_{S_2, H_2}, and disregard the x_ℓ that are not. Since all of the remaining x_ℓ are in U_{S_1, H_1}, we have $U_{S_2, H_2} \subset U_{S_1, H_1}$ and hence H_1 is a quotient of H_2. Also note $U_{S_2, H_2} \subset C_2$. We continue this process and then consider the profinite group H that is the inverse limit of the H_i's. Since $H \in U_{S_\ell, H_\ell} \subset C_\ell \subset B_\ell$ for all ℓ, we have a point $H \in \cap_{\ell \geq 1} B_\ell$ which is a contradiction. □

10. Proof of Theorem 1.1

The last section established the existence of the probability measure μ_u on Borel sets of $\mathcal{P}$. Now we are able to give the proof of Theorem 1.1, the weak convergence of the $\mu_{u,n}$ to μ_u.

Proof of Theorem 1.1. Note that the weak convergence $\mu_{u,n} \Rightarrow \mu_u$ is equivalent to that

$$\liminf_{n \to \infty} \mu_{u,n}(U) \geq \mu_u(U)$$

for all open sets U. In the topological space $\mathcal{P}$, every open set is a countable disjoint union of basic open sets, since two open basic open sets having nontrivial intersection implies that one basic open set contains the other. Assume $U = \cup_{i \geq 1} U_i$ is an open set, where U_i are disjoint basic open sets. By Fatou's lemma, we have

$$\mu_u(U) = \sum_{i \geq 1} \mu_u(U_i) = \sum_{i \geq 1} \lim_{n \to \infty} \mu_{u,n}(U_i) \leq \liminf_{n \to \infty} \sum_{i \geq 1} \mu_{u,n}(U_i) = \liminf_{n \to \infty} \mu_{u,n}(U).$$

□

11. For arbitrary set S

In this section, we let S be an arbitrary (not necessarily finite) set of finite groups and consider the value of μ_u on the specific type of Borel sets

$$V_{S,H} := \{X \in \mathcal{P} \mid X^{\bar{S}} \simeq H\}$$

for a finite level S group H. We will first prove an analogue of Theorem 8.1 for an arbitrary set S (see Theorem 11.4), the proof of which shows that Equation (8.3) gives the value $\mu_u(V_{S,H})$.

Note that $V_{S,H}$ is not a basic open set, but is the intersection of a sequence of basic open sets. Since we will approximate S by increasing finite subsets, we need the following lemma.

Lemma 11.1. *Consider two sets $T \subset T'$ of finite groups. For any positive integer n, finite group H of level T, and $G \in \mathcal{A}_H \cup \mathcal{N}$, we have $m(T, n, H, G) \leq m(T', n, H, G)$. Also if $T_1 \subset T_2 \subset \cdots$ are finite sets of finite groups, then $m(T_m, n, H, G)$ eventually stabilizes as $m \to \infty$.*

Proof. Consider the case when G is abelian. Let $\rho : \hat{F}^{\bar{T}_m} \to H$ be a surjection. Corollary 8.8 and Proposition 8.6 give

$$\frac{h_H(G)^{m(T_m,n,H,G)} - 1}{h_H(G) - 1} = \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E,\pi) \\ \ker \pi \simeq G \text{ as an } H\text{-group} \\ E \text{ is level } T_m}} \frac{|\operatorname{Sur}(\rho,\pi)|}{|\operatorname{Aut}_H(E,\pi)|}.$$

The right-hand side is clearly non-decreasing in m. There are only finitely many isomorphism classes of H-extensions whose kernel is isomorphic to G, which proves the stabilization. The case of non-abelian G is similar. $\qquad\square$

Definition. Let S be a set of finite groups, n a positive integer, and H a finite level S group. Let $T_1 \subset T_2 \subset \cdots$ be finite sets of finite groups such that $\cup_{m\geq1}T_m = S$. For any $G \in \mathcal{A}_H \cup \mathcal{N}$, we define $m(S,n,H,G) = \lim_{m\to\infty} m(T_m,n,H,G)$.

Remark 11.2. It's clear that $m(S,n,H,G)$ does not depend on the choice of the increasing sequence T_i, and $m(S,n,H,G)$ is always a non-negative integer.

It is actually easier to determine $\mu_u(V_{S,H})$, as we will in the next lemma, than to find $\lim_{n\to\infty} \mu_{u,n}(V_{S,H})$, which we will do in Theorem 11.4.

Lemma 11.3. *Let S be a set of finite groups. Let $T_1 \subset T_2 \subset \cdots$ be finite sets of finite groups such that $\cup_{m\geq1}T_m = S$. Let H be a finite group of level S. Let u be an integer. Then*

$$\mu_u(V_{S,H}) = \lim_{m\to\infty}\lim_{n\to\infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H)$$

$$= \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{G\in\mathcal{A}_H} \prod_{i=1}^{\infty}(1 - \lambda(S,H,G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G\in\mathcal{N}} e^{-|G|^{-u}\lambda(S,H,G)}.$$

Proof. First of all, since μ_u is a measure and the sequence $U_{T_m,H^{\bar{T}_m}}$ is descending, we have

$$\mu_u(V_{S,H}) = \mu_u(\cap_{m\geq1}U_{T_m,H^{\bar{T}_m}}) = \lim_{m\to\infty} \mu_u(U_{T_m,H^{\bar{T}_m}}) = \lim_{m\to\infty}\lim_{n\to\infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H).$$

By definition, we have that $\lambda(T,H,G)$ is non-decreasing in T, i.e. if $T \subset T'$ then $\lambda(T,H,G) \leq \lambda(T',H,G)$. Further, again by definition, we have

$$\lambda(S,H,G) = \lim_{m\to\infty} \lambda(T_m,H,G).$$

When m is sufficiently large such that H is level T_m, we have

$$\lim_{n\to\infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H)$$

$$= \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{G\in\mathcal{A}_H} \prod_{i=1}^{\infty}(1 - \lambda(T_m,H,G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G\in\mathcal{N}} e^{-|G|^{-u}\lambda(T_m,H,G)}$$

by Equation (8.3) since T_m is finite. For each $G \in \mathcal{A}_H$, the factor

$$\prod_{i=1}^{\infty}(1 - \lambda(T_m,H,G)\frac{h_H(G)^{-i}}{|G|^u})$$

28

is a limit of terms

$$\prod_{i=1}^{m(T_m,n,H,G)} (1 - \frac{h_H(G)^{m(T_m,n,H,G)} h_H(G)^{-i}}{|G|^{n+u}})$$

by Lemma 8.11, each of which is a probability (see Corollary 5.10) and hence in the interval $[0,1]$. Since the factors

$$\prod_{i=1}^{\infty}(1 - \lambda(T_m, H, G)\frac{h_H(G)^{-i}}{|G|^u}) \qquad \text{and} \qquad e^{-|G|^{-u}\lambda(T_m,H,G)}$$

are all in $[0,1]$ and are non-increasing in m, we have the second equality in the following

$$\lim_{m\to\infty}\lim_{n\to\infty} \mathrm{Prob}((X_{u,n})^{\bar{T}_m} \simeq H)$$

$$= \lim_{m\to\infty} \frac{1}{|\mathrm{Aut}(H)||H|^u} \prod_{G\in\mathcal{A}_H} \prod_{i=1}^{\infty}(1 - \lambda(T_m, H, G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G\in\mathcal{N}} e^{-|G|^{-u}\lambda(T_m,H,G)}$$

$$= \frac{1}{|\mathrm{Aut}(H)||H|^u} \prod_{G\in\mathcal{A}_H} \lim_{m\to\infty}\prod_{i=1}^{\infty}(1 - \lambda(T_m, H, G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G\in\mathcal{N}} \lim_{m\to\infty} e^{-|G|^{-u}\lambda(T_m,H,G)}$$

$$= \frac{1}{|\mathrm{Aut}(H)||H|^u} \prod_{G\in\mathcal{A}_H} \prod_{i=1}^{\infty}(1 - \lambda(S, H, G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G\in\mathcal{N}} e^{-|G|^{-u}\lambda(S,H,G)}.$$

The last equality uses the continuity from Lemma 8.11. $\qquad\square$

Theorem 11.4. *The statement in Theorem 8.1 also works for an arbitrary set S of finite groups.*

Proof. Let T_m be the subset of S of all groups of order at most m in S. Since H is level S, for large enough m we have that $H^{\bar{T}_m} = H$, and from now on we only consider m this large. We can show that $G^{\bar{S}} \simeq H$ if and only if for every $m \geq 1$ we have $G^{\bar{T}_m} \simeq H^{\bar{T}_m}$. Since $G^{\bar{T}_m}$ is a quotient of $G^{\bar{S}}$, the "only if" direction is clear. If we take the inverse limit of the sets $\mathrm{Isom}(G^{\bar{T}_m}, H^{\bar{T}_m})$, with the natural maps, we have an inverse limit of non-empty finite sets, which is non-empty. An element of this inverse limit gives us an isomorphism $G^{\bar{S}} \simeq H^{\bar{S}}$.

From this, and the basic properties of a measure, and Equation (8.2) for finite S, we have that

$$\mathrm{Prob}((X_{u,n})^{\bar{S}} \simeq H)$$

$$= \lim_{m\to\infty} \frac{|\mathrm{Sur}(\hat{F}_n, H)|}{|\mathrm{Aut}(H)||H|^{n+u}} \prod_{G\in\mathcal{A}_H} \prod_{k=0}^{m(T_m,n,H,G)-1} (1 - \frac{h_H(G)^k}{|G|^{n+u}}) \prod_{G\in\mathcal{N}} (1 - |G|^{-n-u})^{m(T_m,n,H,G)}.$$

From Lemma 11.1, we have that

$$\prod_{k=0}^{m(T_m,n,H,G)-1} (1 - \frac{h_H(G)^k}{|G|^{n+u}}) \qquad \text{and} \qquad (1 - |G|^{-n-u})^{m(T_m,n,H,G)}$$

are non-increasing in m, and as they are probabilities they are in the interval $[0,1]$. Thus it follow from basic analysis that

$$\mathrm{Prob}((X_{u,n})^{\bar{S}} \simeq H)$$

$$= \frac{|\operatorname{Sur}(\hat{F}_n, H)|}{|\operatorname{Aut}(H)||H|^{n+u}} \prod_{G \in \mathcal{A}_H} \lim_{m \to \infty} \prod_{k=0}^{m(T_m, n, H, G)-1} (1 - \frac{h_H(G)^k}{|G|^{n+u}}) \prod_{G \in \mathcal{N}} \lim_{m \to \infty} (1 - |G|^{-n-u})^{m(T_m, n, H, G)}$$

By definition of $m(S, n, H, G)$, we have that $\lim_{m \to \infty} m(T_m, n, H, G) = m(S, n, H, G)$ (and the latter is finite). Thus, we have

$$\operatorname{Prob}((X_{u,n})^{\bar{S}} \simeq H)$$

$$= \frac{|\operatorname{Sur}(\hat{F}_n, H)|}{|\operatorname{Aut}(H)||H|^{n+u}} \prod_{G \in \mathcal{A}_H} \prod_{k=0}^{m(S, n, H, G)-1} (1 - \frac{h_H(G)^k}{|G|^{n+u}}) \prod_{G \in \mathcal{N}} (1 - |G|^{-n-u})^{m(S, n, H, G)},$$

which is Equation (8.2) for arbitrary S.

Next, towards Equation (8.3) for arbitrary S, we will show that the order of the limits in Lemma 11.3 could be exchanged.

For every m, we have $\operatorname{Prob}((X_{u,n})^{\bar{S}} \simeq H) \leq \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H)$ and so

$$\limsup_{n \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{S}} \simeq H)$$

$$\leq \lim_{m \to \infty} \lim_{n \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H)$$

(11.5)
$$= \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{G \in \mathcal{A}_H} \prod_{i=1}^{\infty} (1 - \lambda(S, H, G) \frac{h_H(G)^{-i}}{|G|^u}) \prod_{G \in \mathcal{N}} e^{-|G|^{-u} \lambda(S, H, G)}.$$

From here we consider two cases. Case 1 will be the following:

$$\sum_{G \in \mathcal{A}_H} \frac{\lambda(S, H, G)}{h_H(G)|G|^u} + \sum_{G \in \mathcal{N}} \frac{\lambda(S, H, G)}{|G|^u} \quad \text{diverges.}$$

In case 1, the product in Equation (11.5) is 0, and we have proven $\lim_{n \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{S}} \simeq H) = 0$, establishing Equation (8.3).

Case 2 will be the following:

$$\sum_{G \in \mathcal{A}_H} \frac{\lambda(S, H, G)}{h_H(G)|G|^u} + \sum_{G \in \mathcal{N}} \frac{\lambda(S, H, G)}{|G|^u} \quad \text{converges.}$$

We define a *minimal* non-trivial H-extension (E, π) to be an H-extension whose only quotient H-extensions are itself and the trivial one. These are exactly the H-extensions with $\ker \pi$ an irreducible E-group (under conjugation). Also, these are exactly the H-extensions (E, π) such that $\ker \pi$ is an abelian irreducible H-group or $\ker \pi$ is a power of a non-abelian simple group and an irreducible E-group. Since $|\operatorname{Aut}(E)| \geq |\operatorname{Aut}_H(E, \pi)|$ and $h_H(G) \geq 2$, we have

$$\sum_{G \in \mathcal{A}_H} \frac{\lambda(S, H, G)}{h_H(G)|G|^u} + \sum_{G \in \mathcal{N}} \frac{\lambda(S, H, G)}{|G|^u} \geq \frac{1}{2} \sum_{\substack{(E, \pi) \text{ min. non-triv. } H\text{-extension} \\ E \text{ level } S}} |\operatorname{Aut}(E)|^{-1}|G|^{-u}.$$

Since we are in case 2, the sum on the right converges, and

$$\lim_{m \to \infty} \sum_{\substack{(E, \pi) \text{ min. non-triv. } H\text{-extension} \\ E \text{ level } S, \text{ but not level } T_m}} |\operatorname{Aut}(E)|^{-1}|E|^{-u}$$

30

$$= |H|^{-u} \lim_{m \to \infty} \sum_{\substack{(E,\pi) \text{ min. non-triv. } H\text{-extension} \\ E \text{ level } S, \text{ but not level } T_m}} |\operatorname{Aut}(E)|^{-1}|G|^{-u}$$

$$= 0.$$

If $(X_{u,n})^{\bar{S}} \not\simeq H$, but $(X_{u,n})^{\bar{T}_m} \simeq H$ for some m, then $X_{u,n}$ has a surjection to H and thus $X_{u,n}$ has a surjection to some minimal non-trivial H-extension (E, π) of level S but not level T_m. Note that

$$\operatorname{Prob}(X_{u,n} \text{ has a surjection to } E) \le \mathbb{E}(\text{quotients of } X_{u,n} \text{ isom. to } E)$$

$$= |\operatorname{Aut}(E)|^{-1}\mathbb{E}(|\operatorname{Sur}(X_{u,n}, E)|)$$

$$= |\operatorname{Aut}(E)|^{-1}\frac{|\operatorname{Sur}(\hat{F}_n, E)|}{|E|^{n+u}}$$

$$\le |\operatorname{Aut}(E)|^{-1}|E|^{-u}.$$

Thus,

$$\operatorname{Prob}((X_{u,n})^{\bar{S}} \simeq H) \ge \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H) - \sum_{\substack{(E,\pi) \text{ min. non-triv. } H\text{-extension} \\ E \text{ level } S, \text{ but not level } T_m}} |\operatorname{Aut}(E)|^{-1}|E|^{-u}$$

and

$$\liminf_{n \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{S}} \simeq H)$$

$$\ge \lim_{n \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H) - \sum_{\substack{(E,\pi) \text{ min. non-triv. } H\text{-extension} \\ E \text{ level } S, \text{ but not level } T_m}} |\operatorname{Aut}(E)|^{-1}|E|^{-u}$$

Now we take a $\lim_{m \to \infty}$ of both sides and conclude Equation (8.3) for arbitrary S. Finally, note that if $m(S, n, H, G) \ne 0$, then $m(T_m, n, H, G) \ne 0$ for some m, and so the last statement of Theorem 8.1 for infinite S follows from the same statement for finite S. $\qquad \square$

Though this doesn't follow from weak convergence (see Proposition 14.2 and Remark 14.3, for example), we see here that μ_u and $\lim_{n \to \infty} \mu_{u,n}$ agree on the $V_{S,H}$.

Corollary 11.6. *Let S be a set of finite groups and H a finite level S group. Then we have*

$$\lim_{n \to \infty} \mu_{u,n}(V_{S,H}) = \mu_u(V_{S,H}).$$

Proof. In the proof of Theorem 11.4, we showed that

$$\lim_{n \to \infty} \lim_{m \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H) = \lim_{m \to \infty} \lim_{n \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H).$$

By Lemma 11.3, the right-hand side in the above equation is $\mu_u(V_{S,H})$. Also, since $\mu_{u,n}$ are measures on $\mathcal{P}$, we have $\lim_{m \to \infty} \operatorname{Prob}((X_{u,n})^{\bar{T}_m} \simeq H) = \mu_{u,n}(V_{S,H})$. $\qquad \square$

12. EXAMPLES OF THE VALUES OF μ_u

In this section, we will apply Theorem 11.4 to compute $\mu_u(A)$ for some interesting Borel sets A.

Example 12.1 (Trivial group)**.** *Let S contain every finite group. Then the trivial group is the only element in $V_{S,1}$. By Lemma 6.1, if (E, π) is an extension of the trivial group such that $\ker \pi$ is irreducible E-group, then E is a finite simple group. Then it follows from the definition of $\lambda(S, H, G)$ that*

$$\lambda(S, 1, G) = \begin{cases} 1 & G \text{ is a non-trivial abelian simple group} \\ |\operatorname{Aut}(G)|^{-1} & G \text{ is a non-abelian simple group} \\ 0 & \text{otherwise,} \end{cases}$$

where in the first case, we use the fact that $h_1(G) - 1 = |\operatorname{Hom}(G, G)| - 1 = |\operatorname{Aut}(G)|$ as G is simple. By Theorem 11.4, we have

$$\mu_u(\text{trivial group}) = \prod_{p \text{ prime}} \prod_{i=u+1}^{\infty} (1 - p^{-i}) \prod_{\substack{G \text{ finite simple} \\ \text{non-abelian group}}} e^{-|G|^{-u}|\operatorname{Aut}(G)|^{-1}}.$$

The above product over prime integers is zero if and only if $u \leq 0$. When $u \geq 1$, by the classification of finite simple groups, the number of finite simple groups of given order is at most 2. Note that $|\operatorname{Aut}(G)| \geq |\operatorname{Inn}(G)| = |G|$ for every non-abelian simple group G. We have

$$\prod_{\substack{G \text{ finite simple} \\ \text{non-abelian group}}} e^{-|G|^{-u}|\operatorname{Aut}(G)|^{-1}} \geq \exp\Big(- \sum_{\substack{G \text{ finite simple} \\ \text{non-abelian group}}} |G|^{-u-1}\Big) > 0,$$

which shows that $\mu_u(\text{trivial group}) > 0$ if and only if $u \geq 1$. By using the classification of finite simple groups, we are able to give the following approximations

$$\mu_u(\text{trivial group}) \approx \begin{cases} 0.4357 & \text{when } u = 1 \\ 0.7168 & \text{when } u = 2 \\ 0.8616 & \text{when } u = 3. \end{cases}$$

We observe that the product over non-abelian factors is very close to 1 and cannot be seen in this many digits.

Example 12.2 (Any infinite group)**.** *Again let S contain all finite groups. Let H be an infinite profinite group in $\mathcal{P}$, and H_ℓ denote the pro-$\bar{S}_\ell$ completion of H. Since U_{S_ℓ, H_ℓ} is a sequence of basic opens that is decreasing in ℓ and $\cap_\ell U_{S_\ell, H_\ell} = \{H\}$, we obtain*

$$\begin{aligned} \mu_u(\{H\}) &= \lim_{\ell \to \infty} \mu_u(U_{S_\ell, H_\ell}) \\ &\leq \lim_{\ell \to \infty} \frac{1}{|\operatorname{Aut}(H_\ell)||H_\ell|^u}. \end{aligned}$$

Note that H is the inverse limit of H_ℓ, so $\lim_{\ell \to \infty} |H_\ell| = \infty$. It follows that $\mu_u(\{H\}) = 0$ when $u \geq 1$. When $u = 0$, since $\{H\}$ is contained in the Borel set $A := V_{\{\text{all abelian groups}\}, H^{ab}}$ and $\mu_0(A) = 0$ (see Example 12.4), we have $\mu_0(\{H\}) = 0$.

Example 12.3 (Pro-p abelianization)**.** *Let p be a prime integer and S the set consisting of all finite abelian p-groups. Then $\bar{S} = S$ and $(\mathbb{Z}/p\mathbb{Z}, 1)$ is the only element in $\mathcal{CF}(\bar{S})$. Let H be a finite abelian p-group of generator rank d. Then for any $G \in \mathcal{A}_H \cup \mathcal{N}$, the factor in Theorem 8.1 associated to G is 1, unless $G = \mathbb{Z}/p\mathbb{Z}$ with the trivial H-action. We consider the Borel set $V_{S,H}$ that is the set of all profinite groups whose maximal abelian pro-p*

quotient is H. For any integer $n \geq d$, there is a normal subgroup N of $(\hat{F}_n)^{\bar{S}} = (\mathbb{Z}_p)^n$ such that the corresponding quotient is H. Since H is finite, N is isomorphic to $(\mathbb{Z}_p)^n$ with the trivial $(\hat{F}_n)^{\bar{S}}$-action, which shows that $m(S, n, H, \mathbb{Z}/p\mathbb{Z}) = n$ and $\lambda(S, H, \mathbb{Z}/p\mathbb{Z}) = 1$. By Lemma 11.3, we have

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{i=1}^{\infty}(1 - p^{-i-u}).$$

When $u < 0$, this probability is 0, which is as expected since we can never get a finite quotient of $(\mathbb{Z}_p)^n$ with fewer than n relators. When $u \geq 0$, we get a finite group with probability 1. When $u = 0$ or 1, these are the measures used in the Cohen-Lenstra heuristics for class groups of quadratic number fields.

More generally, let's consider an infinite abelian pro-p group H in $\mathcal{P}$. Since $H \in \mathcal{P}$, the pro-$\overline{\{\mathbb{Z}/p\mathbb{Z}\}}$ completion of H is finite, so H is finitely generated, i.e. $H = H_1 \times (\mathbb{Z}_p)^r$ for a finite abelian p-group H_1 and a positive integer r. Let $T_j := \{\mathbb{Z}/p^j\mathbb{Z}\}$. So $\bar{T}_j$ is an increasing sequence and $\cup \bar{T}_j = S$. Assume $n \geq d$ and j is greater than the exponent of H_1. Then we have

$$(\hat{F}_n)^{\bar{T}_j} = (\mathbb{Z}/p^j\mathbb{Z})^n \text{ and } H^{\bar{T}_j} = H_1 \times (\mathbb{Z}/p^j\mathbb{Z})^r.$$

So $m(T_j, n, H, \mathbb{Z}/p\mathbb{Z}) = n - r$, $\lambda(T_j, H, \mathbb{Z}/p\mathbb{Z}) = p^{-r}$ and

$$\begin{aligned}
\mu_u(V_{T_j,H}) &= \frac{1}{|\operatorname{Aut}(H^{\bar{T}_j})||H_1|^u p^{jru}} \prod_{i=1+u+r}^{\infty}(1 - p^{-i}) \\
&= \frac{1}{|\operatorname{Aut}(H_1)||H_1|^{2r+u} p^{jr(r+u)}} \prod_{i=1}^{r}(1 - p^{-i})^{-1} \prod_{i=1+u+r}^{\infty}(1 - p^{-i}),
\end{aligned}$$

since

$$|\operatorname{Aut}(H^{\bar{T}_j})| = |\operatorname{Aut}(H_1)||H_1|^{2r} p^{jr^2} \prod_{i=1}^{r}(1 - p^{-i}).$$

It follows that $\mu_u(V_{S,H}) = \lim_{j\to\infty}(V_{T_j,H}) > 0$ if and only if $u + r = 0$, in which case

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H_1)||H_1|^{-u}} \prod_{i=1-u}^{\infty}(1 - p^{-i}).$$

So we see that when $u < 0$, $\mu_u(V_{S,H}) > 0$ if and only if the (torsion-free) rank of H is $-u$ and we get the groups in such form with probability 1.

Example 12.4 (Abelianization). *Similar to the example above, when S is the set of all finite abelian groups and H is a finite abelian group, we have*

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{p \text{ prime}} \prod_{i=1}^{\infty}(1 - p^{-i-u}),$$

which is 0 if $u \leq 0$ and is positive if $u \geq 1$. If $H = H_1 \times (\hat{\mathbb{Z}})^r$, then

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H_1)||H_1|^{-u}} \prod_{p \text{ prime}} \prod_{i=1-u}^{\infty}(1 - p^{-i}) > 0$$

if $u = -r < 0$ and $\mu_u(V_{S,H}) = 0$ otherwise.

In order to consider the pro-p quotients of our random groups, we will first need to recall the definitions of some p-group invariants. Let H be a finite p-group of generator rank d. The relation rank $r(H)$ of H is defined to be the smallest number of relations in a pro-p presentation of H (and also it is known that $r(H) = \dim_{\mathbb{F}_p} H^2(H, \mathbb{Z}/p\mathbb{Z})$). Let $1 \to N \to \hat{F}_d \to H \to 1$ be a presentation of H. Define $N^* := [N, \hat{F}_d] \cdot N^p$. Then N^* is the minimal $\hat{F}_d$-normal subgroup of N such that N/N^* is a finite elementary abelian p-group with trivial $\hat{F}_d/N^*$-action. $\hat{F}_d/N^*$ is called the p-covering group of H, and N/N^* is called the p-multiplicator of H, and $\dim_{\mathbb{F}_p}(N/N^*)$ is called the p-multiplicator rank of H. It is not hard to see that $r(H)$ is the p-multiplicator rank of H.

Lemma 12.5. *Let H be a finite p-group of generator rank d, S the set of all finite p-groups, and G the H-group that is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial H-action. Then $m(S, d, H, G) = r(H)$ and $m(S, n, H, G) = r(H) + n - d$ for every $n \geq d$.*

Proof. Since the intersection of every normal subgroup and the center of a finite p-group is nontrivial, every finite p-group acts trivially on all of its minimal normal subgroups, which implies $\mathcal{CF}(\bar{S}) = \{(\mathbb{Z}/p\mathbb{Z}, 1)\}$. Recall that $m(S, n, H, G)$ is defined to be $\lim_{i \to \infty} m(T_i, n, H, G)$, where T_i is an increasing sequence of finite sets of groups such that $\cup T_i = S$. When i is sufficiently large such that T_i contains the p-covering group of H, the map $\rho : (\hat{F}_d)^{\bar{T}_i} \to H$ factors through the p-covering group of H. Let $1 \to R \to F \to H \to 1$ be the fundamental short exact sequence associated to T_i, d, H. It is not hard to check that R is also the maximal quotient of $\ker \rho$ that is an elementary abelian p-group with the trivial F-action. Therefore, R is the p-multiplicator of H and $m(S, d, H, G) = m(T_i, d, H, G) = r(H)$.

Assume $n \geq d$. We can find a surjection $\rho_1 : \hat{F}_{n+1} \to H$ and generators $x_1, \cdots, x_{n+1}$ of $\hat{F}_{n+1}$ such that $\rho_1(x_{n+1}) = 1$. Let ρ_2 be the restriction of ρ_1 on the subgroup generated by $x_1, \cdots, x_n$. Then $\rho_2 : \hat{F}_n \to H$ is a surjection. Let $1 \to R_1 \to F_1 \xrightarrow{\pi_1} H \to 1$ and $1 \to R_2 \to F_2 \xrightarrow{\pi_2} H \to 1$ be the fundamental short exact sequences associated to $T_i, n+1, H$ and T_i, n, H that arise from ρ_1 and ρ_2 respectively. These constructions allow us to get a surjection $\pi : F_1 \to F_2$ with $\pi_1 = \pi_2 \circ \pi$, and a generator set $y_1, \cdots, y_{n+1}$ of F_1 such that $\pi(y_{n+1}) = 1$. Since $y_{n+1} \in \ker \pi_1$ and F_1 acts trivially on R_1, the subgroup generated by y_{n+1}, which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, is normal in F_1. It implies that $R_1 \simeq R_2 \times \mathbb{Z}/p\mathbb{Z}$ and $m(T_i, n+1, H, G) = m(T_i, n, H, G) + 1$. By induction on n, we finish the proof of the lemma. $\square$

Example 12.6 (Pro-p quotient). *Let H be a finite p-group of generator rank d, and S the set of all finite p-groups, and G the H-group that is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial H-action. Since $\mathcal{CF}(\bar{S}) = (\mathbb{Z}/p\mathbb{Z}, 1)$, we have*

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{i=1}^{\infty} (1 - \frac{\lambda(S, H, G)}{p^{i+u}}).$$

By Equation (8.12) and Lemma 12.5, $\lambda(S, H, G) = p^{r(H)-d}$. So

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{i=1+u-r(H)+d}^{\infty} (1 - p^{-i}),$$

and $\mu_u(V_{S,H}) > 0$ if and only if $u \geq r(H) - d$.

Given u, if $X_{n,u}^{\bar{S}}$ has generator rank d with $d^2/4 \geq d+u$, we have that the $X_{n,u}^{\bar{S}}$ is necessarily infinite by the Golod-Shafarevich inequality. We can see from the pro-p abelianization that we get groups $X_{n,u}^{\bar{S}}$ with each generator rank $d \geq \min(0, -u)$ with positive probability. All groups in $\mathcal{P}$ have their pro-p quotient finitely generated.

Example 12.7 (Pro-nilpotent quotient)**.** *When S is the set of all finite nilpotent groups and H is a finite nilpotent group with Sylow p-subgroup H_p of generator rank d_p, we have*

$$\mu_u(V_{S,H}) = \frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{p \; prime} \prod_{i=1+u-r(H_p)+d_p}^{\infty} (1 - p^{-i}).$$

Let W be the set of profinite groups G such that there are only finitely many primes p such that the maximal pro-p quotient of G has generator rank $\geq max(2, -u+1)$. By the Borel-Cantelli lemma, we can see that $\mu_u(W) = 1$, and thus μ_u assigns probability 1 to the set of groups who pro-nilpotent quotient is finitely generated.

Example 12.8 (All infinite groups)**.** *When $u \leq 0$, we have $\mu_u(\{infinite\ groups\}) = 1$ (which can already be seen on the abelianization). When $u > 0$, we have $0 < \mu_u(\{infinite\ groups\}) < 1$, since $\mu_u(\{trivial\ group\}) > 0$ and there is positive probability of infinite pro-p quotient. This was seen for the $\mu_{u,n}$ in [JL06].*

13. WHICH GROUPS APPEAR?

In this section, we consider the question of when μ_u is 0 on our basic opens $U_{S,H}$. In order for a basic open $U_{S,H}$ to have positive probability for $\mu_{u,n}$, the group H needs to be able to be generated as a pro-$\bar{S}$ group with n generators and $n + u$ relations. We will see in Proposition 13.4 that the same criterion holds for μ_u. We start with a lemma about the number of generators and relations required to present a pro-$\bar{S}$ group.

Lemma 13.1. *Let S be a finite set of finite groups and u an integer. Let H be a finite pro-$\bar{S}$ group that can be generated by d generators. If H can be presented as a pro-$\bar{S}$ group by m generators and $m + u$ relations, then H can be presented as a pro-$\bar{S}$ group by d generators and $d + u$ relations.*

This is the same as the situation when S is the set of all profinite groups and H is a finite group (see [Lub01, Theorem 0.1]), but contrasts to the more general situation of presenting H as a finite group, where the analog is a long-standing open question (see [Gru76, Lecture 1: Question 3]).

Proof. Suppose for the sake of contradiction that we have a counterexample, and consider one with m minimal. We have that

$$\mu_{u,m}(U_{S,H})$$
$$= \frac{|\operatorname{Sur}(\hat{F}_m, H)|}{|\operatorname{Aut}(H)||H|^{m+u}} \prod_{G \in \mathcal{A}_H} \prod_{k=0}^{m(S,m,H,G)-1} (1 - \frac{h_H(G)^k}{|G|^{m+u}}) \prod_{G \in \mathcal{N}} (1 - |G|^{-m-u})^{m(S,m,H,G)}$$
$$> 0.$$

In particular, since $|G|$ is a power of $h_H(G)$ this implies that for $G \in \mathcal{A}_H$, we have

$$h_H(G)^{m(S,m,H,G)-1}|G|^{-m-u} \leq h_H(G)^{-1}.$$

35

However, since we have a minimal counterexample, we have that $m > d$ and

$$\mu_{u,m-1}(U_{S,H})$$
$$= \frac{|\operatorname{Sur}(\hat{F}_{m-1}, H)|}{|\operatorname{Aut}(H)||H|^{m-1+u}} \prod_{G \in \mathcal{A}_H} \prod_{k=0}^{m(S,m-1,H,G)-1} (1 - \frac{h_H(G)^k}{|G|^{m-1+u}}) \prod_{G \in \mathcal{N}} (1 - |G|^{-m+1-u})^{m(S,m-1,H,G)}$$
$$= 0.$$

By the final statement of Theorem 8.1, we have that one of the factors is 0. Since $m > d$, we have $|\operatorname{Sur}(\hat{F}_{m-1}, H)| \neq 0$. If H is the trivial group, the lemma is clear. Thus we can assume $d \geq 1$ and $m \geq 2$, and so for $G \in \mathcal{N}$ we have $(1 - |G|^{-m+1-u})^{m(S,m-1,H,G)} > 0$. Thus, for some $G \in \mathcal{A}_H$, we have

(13.2)
$$h_H(G)^{m(S,m-1,H,G)-1}|G|^{-m+1-u} \geq 1.$$

If $\rho_n : (\hat{F}_n)^{\bar{S}} \to H$ is a surjection, we have

$$(h_H(G)^{m(S,n,H,G)} - 1)|G|^{-n} = (h_H(G) - 1) \sum_{\substack{\text{isom. classes of } H\text{-extensions } (E, \pi) \\ \ker \pi \simeq G \\ \ker \pi \text{ irred. } E\text{-group} \\ E \text{ is level } S}} \frac{|\operatorname{Sur}(\rho_n, \pi)|}{|\operatorname{Aut}_H(E, \pi)||G|^n}.$$

Any surjection from ρ_n to π can be extended to a surjection from ρ_{n+1} to π in $|G|$ ways. So, $(h_H(G)^{m(S,n,H,G)} - 1)|G|^{-n}$ is non-decreasing in n. So we have

(13.3)
$$\frac{h_H(G)^{m(S,m,H,G)} - 1}{|G|^m} \geq \frac{h_H(G)^{m(S,m-1,H,G)} - 1}{|G|^{m-1}},$$

and then we have

$$|G|^u h_H(G) \leq h_H(G)^{m(S,m-1,H,G)}|G|^{-m+1}$$
$$\leq h_H(G)^{m(S,m,H,G)}|G|^{-m} + |G|^{-m+1} - |G|^{-m}$$
$$\leq |G|^u + |G|^{-m+1} - |G|^{-m},$$

where the first and the last inequalities follow by (13.2) and the second one follows by (13.3). Since $m > d$ and H can be generated by d generators, the number of relations $m+u$ has to be positive. From above, we have $|G|^{m+u}(h_H(G) - 1) \leq (|G| - 1)$. Then this is a contradiction, since $h_H(G) \geq 2$. $\square$

Lemma 13.1 leads to the following definition.

Definition. Let S be a finite set of finite groups and u be an integer. We call a finite group H with generator rank d *achievable* (with S and u implicit) if it can be generated as a pro-$\bar{S}$ group with d generators and $d + u$ relations.

Proposition 13.4. *Let S be a finite set of finite groups and u be an integer. Then for a finite group H we have that $\mu_u(U_{S,H}) > 0$ if H is achievable and $\mu_u(U_{S,H}) = 0$ otherwise.*

So given u, our measure μ_u is supported on those groups in $\mathcal{P}$ whose pro-$\bar{S}$ completion is achievable (for u, S) for every finite set S of finite groups. Note that given S, any finite pro-$\bar{S}$ group H is achievable for u sufficiently large.

Example 13.5. *From* [GKKL07, Theorem A], *we have that every finite simple group can be presented as a profinite group with* 2 *generators and* 18 *relations. Thus if* $u \geq 16$ *and* S *is a finite set of finite groups with* $H \in \bar{S}$ *a simple group, then* H *is achievable.*

Example 13.6. *If* S *is the set of all groups of order* 32 *and* $u \leq 0$, *we can see that* $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *is not achievable. To obtain* H *as a quotient of* F_2, *it is easy to compute we need at least 3 relations (for both generators to be order* 2 *and for them to commute with each other).*

Remark 13.7. Proposition 13.4 need not hold for infinite S. For example, if S is the set of all finite abelian groups, then any finite abelian group H can be presented as an abelian group with n generators and n relations, but $\mu_0(V_{S,H}) = 0$. (See Example 12.4.) This is because the product over $G \in \mathcal{A}_H$ is contains factors $(1 - p^{-1})$ for each prime p and thus is 0 even though no individual factor is 0. Further, if S is the set of all groups and $H \in \mathcal{P}$, we have $\mu_0(V_{S,H}) \leq \mu_0(V_{\{\text{abelian groups}\},H^{ab}}) = 0$. Some of those groups H can be profinitely presented with n generators and n relations. It is an interesting open question to understand in general for which infinite S and finite H does the product in Equation 8.3 give $\mu_u(V_{S,H}) = 0$ even when none of the factors in the product is 0.

Proof of Proposition 13.4. By Lemma 13.1, if H is not achievable, then $\mu_{u,n}(U_{S,H}) = 0$ for all n and hence $\mu_u(U_{S,H}) = 0$. Suppose that $\mu_u(U_{S,H}) = 0$. Then using Theorem 8.1 and Remark 8.4, we must have that one of the factors in

$$\frac{1}{|\operatorname{Aut}(H)||H|^u} \prod_{G \in \mathcal{A}_H} \prod_{i=1}^{\infty} (1 - \lambda(S,H,G)\frac{h_H(G)^{-i}}{|G|^u}) \prod_{G \in \mathcal{N}} e^{-|G|^{-u}\lambda(S,H,G)}.$$

is 0, i.e. for some $G \in \mathcal{A}_H$ we have $\lambda(S,H,G)h_H(G)^{-1}|G|^{-u} \geq 1$. Recall by Remark 5.2 that $|G|$ is a power of $h_H(G)$ and thus so is $\lambda(S,H,G)$. In fact, for sufficiently large n, we have $\lambda(S,H,G) = h_H(G)^{m(S,n,H,G)}|G|^{-n}$. Thus, for sufficiently large n, we have $h_H(G)^{m(S,n,H,G)-1} \geq |G|^{n+u}$ and $\mu_{u,n}(U_{S,H}) = 0$. However if we can present H as a pro-$\bar{S}$ group with d generators and $d + u - k$ relations with $k \geq 0$, we can add m generators for any m and $m + k$ relations to trivialize those generators, to present H with $d + m$ generators and $d + m + u$ relations for all $m \geq 0$, which implies $\mu_{u,n}(U_{S,H}) > 0$ for n sufficiently large. $\square$

14. COMPARISION TO NON-PROFINITE GROUPS

Let $Y_{u,n,\ell}$ be F_n modulo $n + u$ random relations uniform from words of length at most ℓ. In this section, we will compare this model to our $X_{u,n}$. To put the groups on the same footing, we take the profinite completions $\hat{Y}_{u,n,\ell}$ of the $Y_{u,n,\ell}$. Alternatively, we could enlarge our measure space to include non-profinite groups, with the same definition of basic opens. Since our topology would not separate groups with the same profinite completion, we might as well consider only the profinite completions. (Note by [OW11] and [Ago13], at density $< 1/6$, these groups are asymptotically almost surely residually finite and thus inject into their profinite completions.)

The following is almost the same as [DT06, Lemma 4.4], but we include it here for completeness.

Proposition 14.1. *Given integers n, u, we have that the distributions $\nu_{u,n,\ell}$ of the $\hat{Y}_{u,n,\ell}$ weakly converge to $X_{u,n}$.*

Proof. As in the proof of Theorem 1.1, it suffices to show that for each finite group H and finite set S of groups that

$$\lim_{\ell \to \infty} \nu_{u,n,\ell}(U_{S,H}) = \mu_{u,n}(U_{S,H}).$$

Thus we are asked to compare the quotient of the finite group $(\hat{F}_n)^{\bar{S}}$ by the image of random uniform words of length at most ℓ versus by uniform random relators. However as $\ell \to \infty$ the image of a random uniform words of length at most ℓ converges to the uniform distribution on $(\hat{F}_n)^{\bar{S}}$, by the fundamental theorem on irreducible, aperiodic finite state Markov chains [Dur10, Theorem 6.6.4]. □

Next we see that taking a number of relations that is going to infinity always gives groups weakly converging to the trivial group in our topology. This includes all positive density Gromov random groups as well as plenty of density 0 random groups.

Proposition 14.2. *Let $u(\ell)$ be an integer valued function of the positive integers that goes to ∞ as $\ell \to \infty$. Then $\nu_{u(\ell),n,\ell}$ weakly converge to the probability measure supported on the trivial group as $\ell \to \infty$.*

Proof. Fix a finite set S of finite groups and a finite group H. Fix an integer v. For $u(\ell) \geq v$, we have that

$$\mathrm{Prob}(\hat{Y}_{u(\ell),n,\ell} \text{ has a surjection to } H) \leq \mathrm{Prob}(\hat{Y}_{v,n,\ell} \text{ has a surjection to } H).$$

Since the set of groups with a surjection to H is open and closed by Proposition 14.1, we have that

$$\lim_{\ell \to \infty} \mathrm{Prob}(\hat{Y}_{v,n,\ell} \text{ has a surjection to } H) = \mathrm{Prob}(X_{v,n} \text{ has a surjection to } H).$$

It is easy to see using the approach of our paper that

$$\mathbb{E}(|\mathrm{Sur}(X_{v,n}, H)|) = \frac{|\mathrm{Sur}(F_n, H)|}{|H|^{n+v}} \leq |H|^{-v}.$$

Thus

$$\limsup_{\ell \to \infty} \mathrm{Prob}(\hat{Y}_{u(\ell),n,\ell} \text{ has a surjection to } H) \leq |H|^{-v}$$

for every v, and so $\lim_{\ell \to \infty} \mathrm{Prob}(\hat{Y}_{u(\ell),n,\ell} \text{ has a surjection to } H) = 0$. Thus, for every $U_{S,H}$ with H non-trivial, we have that

$$\lim_{\ell \to \infty} \nu_{u(\ell),n,\ell}(U_{S,H}) = 0.$$

For $u(\ell) \geq v$, we have that

$$\mathrm{Prob}(\hat{Y}_{u(\ell),n,\ell}^{\bar{S}} \text{ trivial}) \geq \mathrm{Prob}(\hat{Y}_{v,n,\ell}^{\bar{S}} \text{ trivial}).$$

By Proposition 14.1, we have that

$$\lim_{\ell \to \infty} (\mathrm{Prob}(\hat{Y}_{v,n,\ell}^{\bar{S}} \text{ trivial})) = \mathrm{Prob}(X_{v,n}^{\bar{S}} \text{ trivial}).$$

So

$$\liminf_{\ell \to \infty} \mathrm{Prob}(\hat{Y}_{u(\ell),n,\ell}^{\bar{S}} \text{ trivial}) \geq \limsup_{v \to \infty} \mathrm{Prob}(X_{v,n}^{\bar{S}} \text{ trivial}).$$

38

From Equation (1.2), we have that $\limsup_{v\to\infty} \mathrm{Prob}(X_{v,n}^{\bar{S}}$ trivial$) = 1$. (We can control the size of the product in Equation (1.2), for example, by using the fact that there are at most 2 finite simple groups of any particular order.) Thus, for every $U_{S,1}$, we have that

$$\lim_{\ell\to\infty} \nu_{u(\ell),n,\ell}(U_{S,1}) = 1.$$

$\square$

Remark 14.3. Proposition 14.2 might seem surprising at first. The groups $Y_{u(\ell),n,\ell}$ are plenty interesting as $\ell \to \infty$. In particular they are asymptotically almost surely infinite at density $< 1/2$ [Gro93], and residually finite at density $< 1/6$ [OW11, Ago13], and so have many finite quotients. The above shows that those quotients are escaping off to infinity, however. Just as a very interesting sequence of numbers might go to 0, an interesting sequence of random groups can converge to the trivial group. A better analogy might be that a sequence of integers with interesting asymptotic growth that goes to 0 p-adically. This shows that, at low densities, the weak convergence of $\nu_{u(\ell),n,\ell}$ in ℓ is not as strong as the convergence of the $\mu_{u,n}$ in n that we see in Corollary 11.6. In particular

$$\lim_{\ell\to\infty} \nu_{u(\ell),n,\ell}(\text{trivial group}) = 0 \neq 1.$$

15. List of notations appearing in multiple sections

Notation	§	Description
$\hat{F}_n$	1	Free profinite group on n generators
$X_{u,n}$	1	Random group with n generators and $n+u$ Haar relators
$\mathcal{P}$	1	$\left\{ \text{isom. cl. of profinite groups } G \,\middle|\, \begin{array}{l} \lvert G^{\bar{S}} \rvert < \infty \,\forall \text{ finite set} \\ S \text{ of finite groups} \end{array} \right\}$
$U_{S,H}$	1	Basic open sets: $\{G \in \mathcal{P} \mid G^{\bar{S}} \simeq H\}$ for finite set S
$\mu_{u,n}$	1, 3	distribution of $X_{u,n}$
μ_u	1, 3	probability measure given explicitly, limit of $\mu_{u,n}$
$\mathbf{C}_G(H)$	2.1	Centralizer of a subgroup H of G
$\mathrm{Hom}_F(G_1, G_2)$	2.2	F-group homorphisms $G_1 \to G_2$
$\mathrm{Sur}_F(G_1, G_2)$	2.2	F-group surjections $G_1 \to G_2$
$h_F(G)$	2.2	$\lvert \mathrm{Hom}_F(G,G) \rvert$
$[x_1, \cdots]_F$	2.2	The closed normal F-subgroup of G generated by x_k
(E, π)	2.3	H-extension $\pi : E \to H$
$\mathrm{Sur}_H(\pi, \pi')$	2.3	Surjections between H-extensions
$\mathrm{Aut}_H(E, \pi)$	2.3	Automorphism of an H-extensions (E, π)
$\bar{S}$	2.4	Variety of groups generated by the set S
$G^{\bar{S}}$	2.4	The pro-$\bar{S}$ completion of G
S_ℓ	2.4	$\{$isom. cl. of groups $G \mid \lvert G \rvert \leq \ell\}$
$\mathcal{A}$	3	The algebra of sets generated by basic opens $U_{S,H}$
$\mathcal{A}_H$	3.1	$\{$isom. cl. of non-trivial finite abelian irreducible H-groups$\}$
$\mathcal{N}$	3.1	$\{$isom. cl. of groups G^j for nonabelian simple G and $j \in \mathbb{Z}_{>0}\}$
$\lambda(S, H, G)$	3.1	Values defined for given S, H and G
$1 \to R \to F \to H \to 1$	4	Fundamental short exact sequence
ρ_M	6	$G \to \mathrm{Aut}(M)$ for a minimal normal subgroup M of G

39

$\mathcal{CF}(G), \mathcal{CF}(T)$	6	Chief factor pairs of a group G or a set T
$m(S, n, H, G)$	8	Multiplicity of G in R, see Section 11 for infinite S
$\mathcal{E}_H$	8	poset of H-extensions
$\nu(D, E)$	8	Möbius function on a poset of H-extensions
$V_{S,H}$	11	$\{G \in \mathcal{P} \mid G^{\bar{S}} \simeq H\}$ for arbitrary set S

REFERENCES

[Ago13]   Ian Agol. The virtual Haken conjecture. *Documenta Mathematica*, 18:1045–1087, 2013. With an appendix by Agol, Daniel Groves, and Jason Manning.

[AO96]   G. N. Arzhantseva and A. Yu. Ol′shanskiĭ. Generality of the class of groups in which subgroups with a lesser number of generators are free. Math. Notes **59** (1996), no. 3-4, 350–355; translated from Mat. Zametki **59** (1996), no. 4, 489–496, 638.

[BBH16]   Nigel Boston, Michael R. Bush, and Farshid Hajir. Heuristics for p-class towers of imaginary quadratic fields. *Mathematische Annalen*, pages 1–37, August 2016.

[BW17]   Nigel Boston and Melanie Matchett Wood. Non-abelian Cohen–Lenstra heuristics over function fields. *Compositio Mathematica*, 153(7):1372–1390, July 2017.

[Cha50]   Claude Chabauty. Limite d'ensembles et géométrie des nombres. *Bulletin de la Société Mathématique de France*, 78:143–151, 1950.

[CL84]   Henri Cohen and Hendrik W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number Theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CW15]   Danny Calegari and Alden Walker. Random groups contain surface subgroups. *Journal of the American Mathematical Society*, 28(2):383–419, 2015.

[DT06]   Nathan M. Dunfield and William P. Thurston. Finite covers of random 3-manifolds. *Inventiones mathematicae*, 166(3):457–521, July 2006.

[Dur10]   Rick Durrett. *Probability: Theory and Examples*, volume 31 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, fourth edition, 2010.

[EVW16]   Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological Stability for Hurwitz Spaces and the Cohen-Lenstra Conjecture over Function Fields. *Annals of Mathematics. Second Series*, 183(3):729–786, 2016.

[FJ08]   Michael D. Fried and Moshe Jarden. *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008.

[FK06]   Étienne Fouvry and Jürgen Klüners. Cohen–Lenstra Heuristics of Quadratic Number Fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory*, number 4076 in Lecture Notes in Computer Science, pages 40–55. Springer Berlin Heidelberg, January 2006.

[FW89]   Eduardo Friedman and Lawrence C. Washington. On the distribution of divisor class groups of curves over a finite field. In *Théorie Des Nombres (Quebec, PQ, 1987)*, pages 227–239. de Gruyter, Berlin, 1989.

[GKKL07] Robert Guralnick, William M. Kantor, Martin Kassabov, and Alexander Lubotzky. Presentations of finite simple groups: Profinite and cohomological approaches. *Groups, Geometry, and Dynamics*, 1(4):469–523, 2007.

[Gri84] R. I. Grigorchuk. Degrees of growth of finitely generated groups and the theory of invariant means. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 48(5):939–985, 1984.

[Gro87] M. Gromov. Hyperbolic groups. In *Essays in Group Theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, pages 75–263. Springer, New York, 1987.

[Gro93] M. Gromov. Asymptotic invariants of infinite groups. In *Geometric Group Theory, Vol.\ 2 (Sussex, 1991)*, volume 182 of *London Math. Soc. Lecture Note Ser.*, pages 1–295. Cambridge Univ. Press, Cambridge, 1993.

[Gru76] Karl W. Gruenberg. *Relation Modules of Finite Groups*. American Mathematical Society, Providence, R.I., 1976.

[HB94] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem. II, Invent. Math. **118** (1994), no. 2, 331–370.

[JL06] Moshe Jarden and Alexander Lubotzky. Random normal subgroups of free profinite groups. *Journal of Group Theory*, 2(2):213–224, 2006.

[KK13] M. Kotowski and M. Kotowski, Random groups and property (T): Żuk's theorem revisited, J. Lond. Math. Soc. (2) **88** (2013), no. 2, 396–416.

[Lub01] Alexander Lubotzky. Pro-finite presentations. *Journal of Algebra*, 242(2):672–690, 2001.

[Mac16] John M. Mackay. Conformal dimension via subcomplexes for small cancellation and random groups. *Mathematische Annalen*, 364(3-4):937–982, 2016.

[Neu67] Hanna Neumann. *Varieties of Groups*. Springer-Verlag New York, Inc., New York, 1967.

[Oll05] Yann Ollivier. *A January 2005 Invitation to Random Groups*, volume 10 of *Ensaios Matemáticos [Mathematical Surveys]*. Sociedade Brasileira de Matemática, Rio de Janeiro, 2005.

[Oll10] Yann Ollivier. Random Groups Update January 2010.

[OW11] Yann Ollivier and Daniel T. Wise. Cubulating random groups at density less than 1/6. *Transactions of the American Mathematical Society*, 363(9):4701–4733, 2011.

[Woo15] Melanie Matchett Wood. Random integral matrices and the Cohen Lenstra Heuristics. to appear *American Journal of Mathematics arXiv:1504.04391 [math]*, April 2015.

[Woo17] Melanie Wood. The distribution of sandpile groups of random graphs. *Journal of the American Mathematical Society*, 30(4):915–958, 2017.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN-MADISON, 480 LINCOLN DRIVE, MADISON, WI 53705 USA

E-mail address: `yliu@math.wisc.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN-MADISON, 480 LINCOLN DRIVE, MADISON, WI 53705 USA, AND AMERICAN INSTITUTE OF MATHEMATICS, 600 EAST BROKAW ROAD, SAN JOSE, CA 95112 USA

E-mail address: `mmwood@math.wisc.edu`