STATISTICS OF ISOMORPHISM TYPES IN FREE PRODUCTS

THOMAS W. MÜLLER AND JAN-CHRISTOPH SCHLAGE-PUCHTA

Abstract. Let Γ be a free product of finitely many finite and infinite-cyclic groups. For a subgroup Δ of finite index given by its coset representation we compute its isomorphism type, i.e. its decomposition as a free product of finite and infinite cyclic groups. We determine the set of isomorphism types realized by finite index subgroups, the asymptotics of the subgroup numbers with prescribed isomorphism types, and the distribution of the isomorphism types among subgroups of fixed index. Apart from group-theoretic arguments, the proofs of the present paper make use of asymptotic, and probabilistic ideas and techniques.

1. Introduction

Let

$$\Gamma = G_1 * G_2 * \cdots * G_s * F_r \tag{1}$$

be a free product of finite groups G_σ and a free group F_r of rank r, and let $U_1, \dots, U_t$ be a complete list of isomorphism types of the non-trivial subgroups of $G_1, \dots, G_s$. By the Kuroš Subgroup Theorem, every finite-index subgroup Δ of Γ is of the form

$$\Delta \cong U_1^{*\lambda_1} * U_2^{*\lambda_2} * \cdots * U_t^{*\lambda_t} * F_\mu$$

with non-negative integers $\lambda_1, \dots, \lambda_t, \mu$, and its (rational) Euler characteristics $\chi(\Delta)$ is related to that of Γ via $\chi(\Delta) = (\Gamma : \Delta) \cdot \chi(\Gamma)$. The tuple $\mathbf{t}(\Delta) := (\lambda_1, \dots, \lambda_t; \mu)$ is called the (*isomorphism*) *type* of Δ.

The first aim of the present article is an algorithmic determination of $\mathbf{t}(\Delta)$. In principle, this problem is solved by the Reidemeister-Schreier Theorem; however, this algorithm fails in practice already for quite moderate indices. In algorithmic group theory, a finite-index subgroup Δ is usually represented via the induced action φ_Δ of Γ on the coset space Γ/Δ, and our first main result shows that the isomorphism type of Δ can be immediately read off from this representation.

This algorithmic problem has received considerable attention, and has been solved in various special cases. Millington [8] resolves the case of the modular group $\mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$, while Kulkarni [5] determines the isomorphism types realized by finite-index subgroups in a free product $C_n * C_m$ of two finite cyclic groups. Singerman [18] deals with the analogous problem for Fuchsian groups, thereby in particular resolving the determination problem in the case that all G_σ are cyclic. The methods used in all these approaches are intrinsically geometric, and cannot deal with the general situation addressed here. In [12] a purely group theoretic method was devised to obtain, among other things, an algorithm in the case that all G_σ are cyclic of prime order.

In order to be able to state our result in the general case, let $\rho_{\sigma 1}, \ldots, \rho_{\sigma k_\sigma}$ be a complete list of the transitive permutation representations of G_σ up to similarity, and define the representation type $\mathbf{m}(\Delta)$ of Δ to be the tuple

$$\mathbf{m}(\Delta) = (m_{\sigma\kappa})_{\substack{1 \leq \sigma \leq s\\ 1 \leq \kappa \leq k_\sigma}},$$

where the restriction of φ_Δ to G_σ is similar to $\bigoplus_{\kappa=1}^{k_\sigma} m_{\sigma\kappa}\rho_{\sigma\kappa}$. Our first main result now reads as follows.

Theorem 1. *Let* Γ *be as in* (1), *and let* $\Delta \leq \Gamma$ *be a finite-index subgroup of representation type* $\mathbf{m}(\Delta)$ *and isomorphism type* $\mathbf{t}(\Delta)$. *Then we have*

$$\lambda_\tau = \sum_{\substack{\sigma,\kappa\\ Stab_{\rho_{\sigma\kappa}}(1) \cong U_\tau}} m_{\sigma\kappa} \quad (1 \leq \tau \leq t) \tag{2}$$

and

$$\mu = (r+s-1)(\Gamma : \Delta) - \sum_{\sigma=1}^{s} \sum_{\kappa=1}^{k_\sigma} m_{\sigma\kappa} + 1. \tag{3}$$

¿From an algorithmic point of view, we regard Theorem 1 as a complete solution of the problem of determining the isomorphism type of a subgroup. To make this point more precise, one has to specify the algorithmic problem; that is, one has to define in which way Γ and Δ are given. When doing computations with infinite groups, for example, using GAP [1], a finite-index subgroup of a finitely presented group Γ is given by its coset action, that is, a list $x_1, \ldots, x_k$ of generators of Γ and permutations $\pi_1, \ldots, \pi_k \in S_n$, such that the map $x_i \mapsto \pi_i$ can be extended to a group homomorphism, and $\langle \pi_1, \ldots, \pi_k \rangle$ acts transitively. In view of the normal form of elements in free products it might appear natural to choose generators of the free factors as the generators of Γ; in this case the representation type of Γ can be read off the data structure defining Δ. However, often there are other, equally natural generating sets for Γ. For example, if Γ is a non-cocompact Fuchsian group, one might well prefer parabolic generators over elliptic ones. In this case, to apply the theorem one has to first transform the generating set to obtain a generating set X such that each element in X either has finite order, or generates an infinite cycic free factor of Γ. Of course, this step may be arbitrarily difficult, depending on the actual presentation of Γ, but for reasonable generating sets the effort for the transformation is negligible.

If Δ is defined in some other way, for example, by a generating set, a normal generating set, or as the normalizer of some other subgroup, the computation of the coset representation may become arbitrarily complicated. For this case, computer algebra systems such as GAP [1] have efficient algorithms to compute the coset representation (cf. [2, Section 45.5]).

The proof of Theorem 1 exploits the idea, developed in [11], of relating homomorphisms $\Delta \to H$ for a finite group H to representations of Γ in finite wreath products of the form $H \wr S_n$. Each choice of H yields some information on the isomorphism type of Δ, and the main problem consists in finding an appropriate set of finite groups H determining Δ up to isomorphism. In piecing together these various bits of information, the asymptotics of the function $|\operatorname{Hom}(\Gamma, H \wr S_n)|$, as determined in [11, Theorem 4], plays a crucial rôle. As far as we are aware, Theorem 1 is the first purely group-theoretic application of results in subgroup growth theory. We remark in passing that the methodology of applying wreath product representations to problems of this kind is by no means confined to free products; for instance, Singerman's result mentioned above can be reproved along such lines.

Our principal theme however is different: it centers around the realization problem for isomorphism types as well as their asymptotics and statistics. More explicitly, we shall discuss, for Γ as in (1), the following three basic problems.

(I) (Realization) Which abstract groups admitted by the Kuroš subgroup theorem are realized as finite-index subgroups of Γ?
(II) (Asymptotics) Find a natural domain Ω in $\mathbb{R}^{t+1}$ for $\mathbf{t}$, implying a uniform asymptotics for the function $s_{\mathbf{t}}(\Gamma)$ counting the number of finite-index subgroups in Γ of type $\mathbf{t}$.
(III) (Distribution) What can we say about the distribution of isomorphism types for subgroups of index n in Γ as n tends to infinity?

Originally, the realization problem came up for the modular group and other Hecke groups around 1880 in the work of Klein and Poincaré on automorphic functions; cf., for instance, [3], [4]. Since the early 1960's the general point of view has shifted towards group theory, so that (I)–(III) have become to be regarded as purely algebraic problems in their own right; cf. for instance [7], [8], [15], [16], [17], [19], as well as Newman's monograph [14]. From a recent perspective, a natural context for the research reported in this paper is the theory of *subgroup growth*; for an overview of this fast developing subject see [6].

Using Theorem 1, we can translate the realization problem for isomorphism types into a question concerning existence of permutation representations of prescribed representation type. As a result, we obtain both archimedean and congruence conditions, in fact, there exists a lattice $\Lambda \leq \mathbb{Z}^{t+1}$ and a cone $\mathcal{C}$ over some polytope such that a type $\mathbf{t}$ is realized by some finite-index subgroup Δ if and only if $\mathbf{t} \in \Lambda \cap \mathcal{C}$; cf. Theorem 4.

Permutation representations of given representation type $\mathbf{m}$ are easily counted, and for each transitive permutation representation of type $\mathbf{m}$ we find a subgroup with isomorphism type determined via Theorem 1; hence the only remaining task in solving the asymptotic problem is to compute the proportion of transitive permutation representations among all permutation representations of a given type. This will be accomplished by means of a probabilistic approach, which avoids the heavy computations involved in higher dimensional exponential principles. Our result is as follows.

Theorem 2. *Let Γ be as in* (1)*, let p_σ be the least prime divisor of $|G_\sigma|$, and let $\varepsilon > 0$ be given. Set*

$$\mathcal{M} = \Big\{(\ell_1, \ldots, \ell_s) \in [0,1]^s : \sum_\sigma \min\big(\frac{p_\sigma - 1}{p_\sigma}, 1 - \ell_\sigma\big) > 1 + \varepsilon\Big\},$$

and define

$$\alpha = \sum_\sigma \min\big(\frac{p_\sigma - 1}{p_\sigma}, 1 - \ell_\sigma\big) - 1.$$

Let μ_τ be the number of subgroups isomorphic to U_τ among all subgroups of $G_1, \ldots, G_s$. Let $(\lambda_1, \ldots, \lambda_t; \mu)$ be an isomorphism type. For each $\sigma \leq s$ define $\nu_\sigma = \lambda_\tau$, where τ is the unique index satisfying $G_\sigma = U_\tau$, and let n be the index of a subgroup of type $\mathbf{t}$. Then the asymptotic formula

$$s_{\mathbf{t}}(\Gamma) = \Big(1 + \mathcal{O}\big(n^{-\alpha+\varepsilon}\big)\Big) \frac{n \cdot n!^{s+r-1} \prod_{\tau=1}^t \mu_\tau^{\lambda_\tau}}{\prod_{\tau=1}^t \lambda_\tau! |U_\tau|^{\lambda_\tau}}, \tag{4}$$

holds true uniformly in the set of types $\mathbf{t}$ such that $(\frac{\log \nu_1}{\log n}, \ldots, \frac{\log \nu_s}{\log n}) \in \mathcal{M}$.

Similarly, the problem of determining the asymptotic distribution of isomorphism types is translated via Theorem 1 into the corresponding problem for representation types, and then, by the universal mapping property of free products, into a statistical problem for finite groups. This last problem is solved by applying the method of moments, and we obtain the following.

Theorem 3. *Let Γ be as in* (1), $\chi(\Gamma) < 0$, *let $U_1, \ldots, U_t$ be as above, and let n be a positive integer. Define random variables $\xi_1^{(n)}, \ldots, \xi_t^{(n)}$ by choosing a subgroup Δ of Γ of index n at random (with respect to the uniform distribution), and putting $(\xi_1^{(n)}, \ldots, \xi_t^{(n)}; \mu)$ to be the isomorphism type of Δ. Then the variables $\xi_1^{(n)}, \ldots, \xi_t^{(n)}$ are asymptotically independent. For each τ set $d_\tau = \min_\sigma(G_\sigma : U_\tau)$, the minimum being taken over all σ such that G_σ contains a subgroup isomorphic to U_τ, and let m_τ be the number of subgroups of index d_τ occurring in $G_1, \ldots, G_s$ which are isomorphic to U_τ. Then $\frac{\xi_\tau^{(n)} - m_\tau n^{1/d_\tau}}{\sqrt{m_\tau}\, n^{1/2d_\tau}}$ converges to a standard normal distribution. More precisely, denoting by M_ℓ the ℓ-th moment of $\xi_\tau^{(n)}$ and by $\tilde{M}_\ell$ the ℓ-th moment of the corresponding normal distribution, we have*

$$M_\ell = \big(1 + \mathcal{O}(\ell^2 n^{-1/m_\tau}) + \mathcal{O}(n^{-\alpha})\big)\tilde{M}_\ell$$

uniformly for $r < \sqrt{n}$, where α is as in Theorem 2.

2. Computing the isomorphism type

Our starting point will be the following result.

Proposition 1 (Proposition 1 in [12]). *Let Γ be as in* (1), *let $U_1, \ldots, U_t$ be as above, and let H be a finite group. Then isomorphism and representation type of a subgroup Δ of index n in Γ are related via the equation*

$$\begin{aligned} |H|^{nr} \prod_{\sigma=1}^s \prod_{\kappa=1}^{k_\sigma} \Big|\Big\{\psi \in \mathrm{Hom}(G_\sigma, H \wr S_{d_{\sigma\kappa}}) :\ \pi\psi = \rho_{\sigma\kappa}\Big\}\Big|^{m_{\sigma\kappa}} &= |H|^{n+\mu-1} \\ &\times \prod_{\tau=1}^t |\,\mathrm{Hom}(U_\tau, H)|^{\lambda_\tau}. \end{aligned} \tag{5}$$

Here, π is the canonical projection onto the permutation group. Taking the p-adic valuation, we obtain, for every H and each prime p, a linear relation between $\mathbf{m}(\Delta)$ and $\mathbf{t}(\Delta)$. Our first aim is to show that these equations contain enough information to determine the isomorphism type for fixed representation type. The proof of this result, though constructive in principle, is in itself of little computational value. However, the mere fact that these equations have a unique solution, when coupled with explicit computations in certain special cases, then leads to a set of equations explicitly computing the isomorphism type of Δ in terms of its representation type.

Proposition 2. *Let Γ be as in* (1), *and let Δ_1, Δ_2 be finite-index subgroups of Γ. If Δ_1 and Δ_2 have the same representation type, then they are isomorphic. More precisely there exists a linear map A, such that $A\mathbf{m}(\Delta) = \mathbf{t}(\Delta)$.*

The proof of Proposition 2 requires the following auxiliary result.

Lemma 1. *Let G, G_1, G_2, and H be finite groups.*

(i) *We have*

$$|\operatorname{Hom}(G, H \wr S_n)| = (n!)^{1-1/|G|}\, e^{\mathcal{O}(\sqrt{n})}.$$

(ii) *Suppose that, as $n \to \infty$,*

$$|\operatorname{Hom}(G_1, H \wr S_n)| \sim |\operatorname{Hom}(G_2, H \wr S_n)|.$$

Then these sequences are in fact equal for all n.

Proof. For finite groups G and H we have the following identity of generating series (cf. [11, Example 4]),

$$\sum_{n\geq 1} |\operatorname{Hom}(G, H \wr S_n)| \frac{z^n}{n!} = \exp\left(P_G^H(z)\right),$$

where

$$P_G^H(z) = \sum_{d|m} |H|^{d-1} \sum_{(G:U)=d} |\operatorname{Hom}(U, H)| \frac{z^d}{d}.$$

The first claim is now a crude consequence of [10, Theorem 1], whereas the second statement is implied by the fact, established in [13], that for polynomials $P_1(z)$, $P_2(z)$ the property that the coefficients of the power series of $e^{P_1(z)}$ and $e^{P_2(z)}$ are ultimately positive and asymptotically equal already implies $P_1(z) = P_2(z)$. □

Proof of Proposition 2. The left-hand side of (5) is determined by the representation type of Δ. We claim that as H runs over all finite groups we obtain a system of equations, which is uniquely solvable in the variables μ, λ_τ. From this the proposition follows. In fact, for all H the left-hand side of (5) as well as $|H|$ and $|\operatorname{Hom}(U_\tau, H)|$ are integers, that is, for one group H the single equation (5) is equivalent to the system of linear equations which for each prime number p contains the equation

$$\nu_p(|H|)rn + \sum_{\sigma=1}^{s}\sum_{\kappa=1}^{k_\sigma} \nu_p\Big(\Big|\Big\{\psi \in \mathrm{Hom}(G_\sigma, H \wr S_{d_{\sigma\kappa}}) :\ \pi\psi = \rho_{\sigma\kappa}\Big\}\Big|\Big) m_{\sigma\kappa}$$
$$= \nu_p(|H|)(n+\mu-1) + \sum_{\tau=1}^{t} \nu_p\big(|\,\mathrm{Hom}(U_\tau, H)|\big)\lambda_\tau,$$

where $\nu_p(x)$ is the exponent of p in x, that is, the unique integer e satisfying $p^e|x$, $p^{e+1} \nmid x$. Hence, if the system consisting of equation (5) for each finite group H is uniquely solvable, then the variables λ_τ are the unique solution of a linear system of equations, where the inhomogenity is a linear function of the parameters $m_{\sigma\kappa}$. But then the unique solution can be obtained by applying some linear map to the parameters.

By [12, Prop. 3], the parameter μ is given as

$$\mu = (r+s-1)n - \sum_{\sigma=1}^{s}\sum_{\kappa=1}^{k_\sigma} m_{\sigma\kappa} + 1,$$

which is obviously linear, hence, it remains to show that the variables λ_τ are uniquely determined by the equations (5) for all finite groups H.

Let H be a finite group, p a prime number. Replacing H by $C_p \wr H$ in (5), and computing the second factor of the right hand side of this equation, we see that the representation type determines

$$\prod_{\tau=1}^{t}\left(\sum_{\varphi: U_\tau \to H} p^{|H| - |\mathrm{Orbits}(\varphi(U_\tau))|}\right)^{\lambda_\tau} = \prod_{\tau=1}^{t}\left(\sum_{U \leq H} |\mathrm{Epi}(U_\tau, U) p^{|H|-(H:U)}\right)^{\lambda_\tau},$$

where $\mathrm{Orbits}(\varphi(U_\tau))$ denotes the set of domains of transitivity of the action of U_τ induced by φ. The right-hand side is a polynomial in p of degree $\leq (|H|-1)\sum_i \lambda_\tau$, hence choosing for p sufficiently many prime numbers, we see that the representation type determines the polynomial itself. Replacing p by the variable X, dividing by $X^{|H|\sum_i \lambda_\tau}$, and replacing X by $1/X$, we see that for every H, the representation type determines the polynomial

$$\prod_{\tau=1}^{t}\left(\sum_{U \leq H} |\mathrm{Epi}(U_\tau, U)| X^{(H:U)}\right)^{\lambda_\tau}.$$

Setting $H \wr S_n$ for H in the last expression, and replacing X by $X^{m_\Gamma/|H \wr S_n|}$, where m_Γ is the least common multiple of all $|G_\sigma|$, we find that for every finite group H, the representation type determines the polynomial

$$\prod_{\tau=1}^{t}\left(\sum_{U} |\mathrm{Epi}(U_\tau, U)|\, |\mathrm{Mono}(U, H \wr S_n)| X^{m_\Gamma/|U|}\right)^{\lambda_\tau},$$

where the sum is formally taken over the isomorphism types of all finite groups. Let

$$P_{\tau,n}(X) = \sum_{U} |\mathrm{Epi}(U_\tau, U)|\, |\mathrm{Mono}(U, H \wr S_n)| X^{m_\Gamma/|U|}.$$

We want to approximate these polynomials by simpler expressions; to do this, let o_τ be the order of the largest proper quotient of U_τ. Define the polynomial $Q_{\tau,n}$ via

$$\begin{aligned} Q_{\tau,n}(X) &= |\mathrm{Aut}(U_\tau)|\cdot|\mathrm{Mono}(U_\tau, H\wr S_n)|X^{m_\Gamma/|U_\tau|}\\ &\quad+\sum_{|U|=o_\tau}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|X^{m_\Gamma/|U|}\\ &= |\mathrm{Aut}(U_\tau)|\cdot|\mathrm{Mono}(U_\tau, H\wr S_n)|X^{m_\Gamma/|U_\tau|}\\ &\quad\times\left(1+\frac{\sum_{|U|=o_\tau}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|}{|\mathrm{Aut}(U_\tau)|\cdot|\mathrm{Mono}(U_\tau,H\wr S_n)|}X^{m_\Gamma/o_\tau-m_\Gamma/|U_\tau|}\right).\end{aligned}$$

For each complex $(\frac{m_\Gamma}{o_\tau}-\frac{m_\Gamma}{|U_\tau|})$-th root ζ of -1, $Q_{\tau,n}$ has a simple zero at

$$z_{0,\tau}=\zeta\cdot\left(\frac{\sum_{|U|=o_\tau}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|}{|\mathrm{Aut}(U_\tau)|\cdot|\mathrm{Mono}(U_\tau,H\wr S_n)|}\right)^{\overline{\frac{1}{(\frac{m_\Gamma}{o_\tau}-\frac{m_\Gamma}{|U_\tau|})}}}$$

Since the order of U_τ is strictly larger then o_τ, applying the first part of Lemma 1, we find that, as $n\to\infty$, the sequence $|\mathrm{Mono}(U_\tau,H\wr S_n)|$ is of larger growth than $|\mathrm{Mono}(U,H\wr S_n)|$ for every finite group U of order o_τ; hence, $z_{0,\tau}\to 0$. For $|z-z_{0,\tau}|=\frac{|z_{0,\tau}|}{n}$ and $n\to\infty$, we have

$$\begin{aligned}|Q_{\tau,n}(z)| &\gg n^{-1}|\mathrm{Aut}(U_\tau)|\cdot|\mathrm{Mono}(U_\tau,H\wr S_n)|\cdot|z_{0,\tau}|^{m_\Gamma/|U_\tau|}\\ &\gg (n!)^{1-1/|U_\tau|-\varepsilon}\,|z_{0,\tau}|^{m_\Gamma/|U_\tau|},\end{aligned}$$

whereas for $|z|\leq 2|z_{0,\tau}|$, we have

$$\begin{aligned}|P_{\tau,n}(z)-Q_{\tau,n}(z)| &\leq \sum_{|U|<o_\tau}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|\cdot|z_{0,\tau}|^{m_\Gamma/(o_\tau-1)}\\ &\ll |H|^n\,|z_{0,\tau}|^{m_\Gamma/(o_\tau-1)}\sum_{|U|<o_\tau}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Hom}(U,S_n)|\\ &\ll |H|^n\,|z_{0,\tau}|^{m_\Gamma/(o_\tau-1)}\,(n!)^{1-1/(o_\tau-1)+\varepsilon},\end{aligned}$$

and, for n sufficiently large, we deduce from Rouché's theorem that $P_{\tau,n}$ has some root $z_{1,\tau}$ with $|z_{0,\tau}-z_{1,\tau}|\leq\frac{|z_{0,\tau}|}{n}$. Note that for n sufficiently large we have $|z_{1,\tau}|<1$.

Now assume that there are two different tuples $(\lambda_1,\dots,\lambda_t)$, $(\lambda_1',\dots,\lambda_t')$, such that the polynomials $\prod_{\tau=1}^t P_{\tau,n}(X)^{\lambda_\tau}$ and $\prod_{\tau=1}^t P_{\tau,n}(X)^{\lambda_\tau'}$ coincide. Without loss we may assume that $\lambda_1\neq\lambda_1'$, and that the order of U_1 is maximal among all τ with $\lambda_\tau\neq\lambda_\tau'$. Then, for each root z_0 of $P_{1,n}$, there is some $\tau\neq 1$, such that $\lambda_\tau\neq\lambda_\tau'$, and z_0 is a root of $P_{\tau,n}$. In particular, for some $\tau>1$, we have $z_{1,1}=z_{1,\tau}$. Suppose that there exist infinitely many integers n, such that

$$\sum_U|\mathrm{Epi}(U_1,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|\neq\sum_U|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|. \tag{6}$$

Let k be the largest integer such that

$$\sum_{|U|=k}|\mathrm{Epi}(U_1,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|\neq\sum_{|U|=k}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|$$

for infinitely many n, and let n tend to infinity through a set of integers such that the last relation holds true. Then we have

$$\begin{aligned}
0 &= P_{1,n}(z_{1,1}) - P_{\tau,n}(z_{1,1})\\
&= \sum_{\kappa\leq k}\left(\sum_{|U|=\kappa}\Big(|\mathrm{Epi}(U_1,U)| - |\mathrm{Epi}(U_\tau,U)|\Big)\,|\mathrm{Mono}(U,H\wr S_n)|\right) z_{1,1}^{m_\Gamma/k}\\
&= \left(\sum_{|U|=k}\Big(|\mathrm{Epi}(U_1,U)| - |\mathrm{Epi}(U_\tau,U)|\Big)\,|\mathrm{Mono}(U,H\wr S_n)|\right) z_{1,1}^{m_\Gamma/k}\\
&\quad + \mathcal{O}\big(|H|^n n!^{1-1/(k-1)+\varepsilon}|z_{1,1}|^{m_\Gamma/(k-1)}\big).
\end{aligned}$$

Since $|\mathrm{Mono}(U,H\wr S_n)| \gg |\mathrm{Hom}(U,S_n)| \gg n!^{1-1/|U|-\varepsilon}$, and $|z_{1,1}|<1$, we deduce that

$$\sum_{|U|=k}|\mathrm{Epi}(U_1,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)| \sim \sum_{|U|=k}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|.$$

If there are only finitely many integers n satisfying (6), this asymptotics holds trivially. Lemma 1 now implies that these functions coincide for all n. Hence, we obtain that, for every finite group H, there is some τ such that

$$\sum_{|U|=k}|\mathrm{Epi}(U_1,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)| = \sum_{|U|=k}|\mathrm{Epi}(U_\tau,U)|\cdot|\mathrm{Mono}(U,H\wr S_n)|$$

for all n and k. Setting $n=1$ and summing over all k, we deduce that $|\operatorname{Hom}(U_1,H)| = |\operatorname{Hom}(U_\tau,H)|$ for all finite groups H. Sifting over subgroups of H, we deduce that $|\operatorname{Epi}(U_1,H)| = |\operatorname{Epi}(U_\tau,H)|$ as well, in particular, $|\operatorname{Epi}(U_\tau,U_1)|\geq 1$. Since by assumption $|U_1|\geq|U_\tau|$, we obtain $U_1\cong U_\tau$, contrary to our assumption $\tau>1$. □

To prove Theorem 1, we first need to establish the following special case.

Lemma 2. *Let p be a prime and let $k\geq 2$ be an integer. Then the assertion of Theorem 1 holds for groups Γ of the form $C_p^{*e_1} * C_{p^k}^{*e_2} * F_r$.*

Proof. We apply Proposition 1 with $H=C_{p^i}$, $1\leq i\leq k$. Denote by ρ_{11} the trivial representation, by ρ_{12} the regular representation of C_p, and by ρ_{2j} the representation of C_{p^k} on p^{j-1} points. Then we have

$$\begin{aligned}
\Big|\Big\{\psi\in\mathrm{Hom}(C_p, C_{p^i}\wr S_1):\ \pi\psi=\rho_{11}\Big\}\Big| &= p\\
\Big|\Big\{\psi\in\mathrm{Hom}(C_p, C_{p^i}\wr S_p):\ \pi\psi=\rho_{12}\Big\}\Big| &= p^{i(p-1)}\\
\Big|\Big\{\psi\in\mathrm{Hom}(C_{p^k}, C_{p^i}\wr S_{p^{j-1}}):\ \pi\psi=\rho_{2j}\Big\}\Big| &= p^{i(p^{j-1}-1)+\min(k-j-1,i)},\quad 1\leq j\leq k+1,
\end{aligned}$$

as well as

$$|\operatorname{Hom}(C_p,C_{p^i})| = p \quad\text{and}\quad |\operatorname{Hom}(C_{p^k},C_{p^i})| = p^{\min(i,k)}.$$

Taking logarithm to base p we find that the i-th equation becomes

$$inr + m_{11} + i(p-1)m_{12} + \sum_{j=1}^{k+1} \big(i(p^{j-1}-1) + \min(k-j+1, i)\big)m_{2j}$$
$$= i(n+\mu-1) + \sum_{j=1}^{k} \min(j,i)\lambda_\tau. \quad (6_i)$$

First, we compute $2 \cdot (6_1) - (6_2)$ and obtain $m_{11} + m_{2k} = \lambda_1$. Next we consider $2 \cdot (6_i) - (6_{i-1}) - (6_{i+1})$ for $2 \leq i \leq k-1$, obtaining $m_{2k-i+1} = \lambda_i$. Finally, we insert this information into (6_k) and find that

$$knr - km_{11} + e_1kn - km_{12} + e_2kn - k\sum_{j=1}^{k+1} m_{2j} + m_{2k} = k(n+\mu-1) + k\lambda_k,$$

where we have used the facts that $m_{11}+pm_{12} = e_1n$ and $\sum_{j=1}^{k+1} p^{j-1}m_{2j} = e_2n$. Applying (3), which is part (i) of [12, Prop. 3], we deduce $m_{2k} = \lambda_k$. Hence, our claim is proven. □

Proposition 3. *Let Γ be a split extension of a free group F by a finite group G.*

(i) *If Γ has a finite free factor H, then H is isomorphic to a subgroup of G as well as to a quotient of G. If $H \neq 1, G$, then G has a p-Sylow subgroup of exponent $\geq p^2$ for some prime p.*

(ii) *If Γ decomposes as a free product of finite groups and infinite cyclic groups, and the rank of F is finite, then all finite factors of Γ are isomorphic to G.*

Proof. Write $\Gamma = H * \Gamma'$, and let $\varphi : \Gamma \to H$ be the canonical projection. Then φ factors through F, hence, φ induces a surjective map $\Gamma/F \to H$, thus H is a quotient of G. On the other hand, $HF/F \cong H$, thus H is a subgroup of G. Let G be minimal among all finite groups such that there exists an extension Γ and a finite group $H \neq 1, G$ as above. Let $M < G$ be a maximal subgroup. If $\varphi(MF)$ was not trivial, MN would have a free factor, which is a non-trivial subgroup of H, which contradicts the minimality of G. Hence, $\ker\varphi/F$ contains all maximal subgroups of G, but not G itself, hence G has only one maximal subgroup, and therefore is cyclic of prime power order. Moreover, G has a subgroup $H \not\cong 1, G$, thus $|G| \geq p^2$. Hence, every group G contains a cyclic group of order p^2 for some prime p, which implies our first claim.

Moreover, in a minimal example to the first claim we may suppose that $|H| = p$, for otherwise H would have a proper subgroup U, and $\varphi^{-1}(U)/F$ would be a smaller example. Hence, for the second claim it suffices to consider $G = C_{p^k}$, $H = C_p$ and $\Gamma = C_p^{*e_1} * C_{p^k}^{*e_2} * F_r$, where G is one of the free factors; we have to show that $e_1 = 0$. Suppose otherwise, and consider the projection φ of Γ onto a free factor C_p. Then $\Delta = \ker\varphi$ contains both G and F, in particular, G acts trivially on Γ/Δ, thus, by Lemma 2, Δ has a free factor isomorphic to G. However, Δ/F is a proper subgroup of $\Gamma/F \cong G$, and φ would induce an surjection of a proper subgroup of G onto G, which is absurd. □

Note that in the proof of the second part we have already used Theorem 1, but only in the cases established in Lemma 2. This is important, since we need Proposition 3 to prove Theorem 1 in full generality.

Proof of Theorem 1. Let Δ be a finite-index subgroup of Γ. Relabel the representations $\rho_{\sigma\kappa}$ $(1 \leq \sigma \leq s, 1 \leq \kappa \leq k_\sigma)$ as $\rho_1, \dots, \rho_u$. We know from Proposition 2 that $\mathbf{t}(\Delta)$ is determined by $\mathbf{m}(\Delta)$ using only linear equations. Solving these equations for the isomorphism type leads to a linear map, and we deduce that there exist constants $\alpha_{\tau j}$, $1 \leq \tau \leq t$, $1 \leq j \leq u$, such that

$$\lambda_\tau = \sum_{j=1}^u \alpha_{\tau j} m_j.$$

We claim that

$$\alpha_{\tau j} = \begin{cases} 1, & \mathrm{Stab}_{\rho_j}(1) \cong U_\tau \\ 0, & \text{otherwise} \end{cases}, \tag{7}$$

which implies our claim. Let N be the kernel of the map $\varphi : \Gamma \to G_1 \times G_2 \times \ldots \times G_s$, fix a subgroup U_τ and a representation ρ_j of G_1, say. Set $H = \mathrm{stab}_{\rho_j}(1)$, and let $\Delta \geq N$ be the subgroup of Γ, such that

$$\varphi(\Delta) = H \times 1 \cdots \times 1.$$

For $\sigma \neq 1$, G_σ acts regularly on the cosets of Δ, whereas the action of G_1 is a multiple of ρ_j. Since Δ is a split extension of the free group N by H, Proposition 3 (ii) implies that U_τ can only occur as a free factor of Δ, if $\mathrm{stab}_{\rho_j}(1) \cong U_\tau$, that is $\alpha_{\tau j} = 0$ for all other pairs τ, j.

If $\mathrm{stab}_{\rho_j} \cong U_\tau$, then $\Delta \cong U_\tau^{*\lambda_\tau} * F_\mu$, and, computing the Euler characteristic, we obtain the equation

$$\lambda_\tau\Big(1 - \frac{1}{|U_\tau|}\Big) + \mu - 1 = \frac{|G_1| \cdots |G_s|}{|U|} \left(\sum_{\sigma=1}^s \Big(1 - \frac{1}{|G_\sigma|}\Big) + r - 1\right),$$

whereas from [12, Proposition 3], we have the equation

$$\mu = \frac{|G_1| \cdots |G_s|(r+s-1)}{|U|} - \sum_{\sigma \geq 2} \frac{|G_1| \cdots |G_s|}{|U_\tau| \cdot |G_\sigma|} - \frac{|G_1| \cdots |G_s|}{|G_1|} + 1,$$

and combining these equations we obtain

$$\lambda_\tau\Big(1 - \frac{1}{|U_\tau|}\Big) = |G_2| \cdots |G_s| - \frac{|G_2| \cdots |G_s|}{|U_\tau|},$$

hence $\lambda_\tau = |G_2| \cdots |G_s|$; that is, in this case we have $\alpha_{\tau j} = 1$. □

3. The realization problem for isomorphism types

Theorem 4. *Let* Γ *be as in* (1), *and let* $\mathbf{t} = (\lambda_1, \dots, \lambda_t; \mu)$ *be a tuple of non-negative integers. Then there exists a finite-index subgroup with isomorphism type* $\mathbf{t}$ *if, and only if, the following two conditions are satisfied.*

(i) *The quantity*
$$n=\frac{\sum_\tau \lambda_\tau\big(1-\frac{1}{|U_\tau|}\big)+\mu-1}{\sum_\sigma\big(1-\frac{1}{|G_\sigma|}\big)+r-1}$$
is a positive integer.

(ii) *There exist non-negative integers $\nu_{\tau\sigma}$, $1\leq\tau\leq t$, $1\leq\sigma\leq s$, such that $\sum_\tau\frac{|G_\sigma|}{|U_\tau|}\nu_{\tau\sigma}\leq n$, $\sum_\sigma\nu_{\tau\sigma}=\lambda_\tau$, and $\nu_{\tau\sigma}=0$ unless U_τ is isomorphic to a subgroup of G_σ, where n is given as in* (i).

Proof. First, we consider necessity. Condition (i) is but a reformulation of the multiplicativity of Euler characteristics. Let Δ be a subgroup with isomorphism type $\mathbf{t}$, and let $\mathbf{m}=(m_{\sigma\kappa})$ be the representation type of Δ. Then by Theorem 1 we have
$$\lambda_\tau=\sum_{\substack{\sigma,\kappa\\ \mathrm{Stab}_{\rho_{\sigma\kappa}}(1)\cong U_\tau}} m_{\sigma\kappa},$$
and since the number of points not contained in regular orbits cannot exceed the total number of points, we have for each σ the inequality
$$\sum_{\kappa=1}^{k_\sigma} d_{\sigma\kappa}m_{\sigma\kappa}\leq n. \tag{8}$$
Hence, setting $\nu_{\tau\sigma}=\sum_{\kappa:\mathrm{Stab}_{\rho_{\sigma\kappa}}(1)\cong U_\tau} m_{\sigma\kappa}$, we have found non-negative integers as required by the second condition. To prove that conditions (i) and (ii) are sufficient, suppose that we are given integers $\nu_{\tau\sigma}$ as in the second condition. For each τ,σ, such that G_σ contains a subgroup isomorphic to U_τ, we choose such a subgroup, which defines a permutation representation $\rho_{\sigma\kappa}$. We put $m_{\sigma\kappa}=\nu_{\tau\sigma}$, and $m_{\sigma\kappa'}=0$ for all $\kappa'\neq\kappa$, for which $\mathrm{Stab}_{\rho_{\sigma\kappa}}(1)\cong U_\tau$.

For this choice of $\mathbf{m}$, Condition (ii) implies (8), and this estimate implies that there exists a permutation representation of type $(m_{\sigma\kappa})$; our task is to construct a transitive permutation representation of this type. If $r\geq 1$ this task is simple, for the action of F_r can be chosen to be transitive, and the action of the finite free factors can be chosen according to $(m_{\sigma\kappa})$. If $r=0$, solving condition (i) for μ and rewriting the λ_τ in terms of the representation type, we obtain
$$\sum_{\sigma=1}^{s}\sum_{\kappa=1}^{k_\sigma}(d_{\kappa\sigma}-1)m_{\sigma\kappa}-n+1=\mu\geq 0,$$
and therefore
$$\sum_{\sigma=1}^{s}\sum_{\kappa=1}^{k_\sigma}(d_{\kappa\sigma}-1)m_{\sigma\kappa}\geq n-1.$$
Intuitively, this inequality shows that we can find a transitive representation of type $(m_{\sigma\kappa})$, since if we choose domains of transitivity for each transitive constituent one after the other in such a way that the total number of orbits is diminished as fast as possible, inserting a domain of size $d_{\kappa\sigma}$ reduces the number of orbits by $d_{\kappa\sigma}-1$. Since we begin with n orbits consisting of 1 point each, we should be able to reach a representation with 1 orbit, that is, a transitive permutation representation of the desired type.

To make this argument precise, we have to show that we can indeed choose representations in such a way that either the number of remaining orbits is diminished by the maximal amount, or we already reach a transitive action at some intermediate stage. Suppose that according to $(m_{\sigma\kappa})$, the number of fixed points of G_1 is minimal among all G_σ, choose the action of G_1 according to $(m_{\sigma\kappa})$, and list the orbits of this action in some way. Let $\Omega_1, \dots, \Omega_\ell$ be the orbits of G_1 of size ≥ 2. To define an action of G_2 with the desired representation type it suffices to choose the domains of transitivity containing ≥ 2 points of this action, so let $d_1, \dots, d_m$ be a list of the occurring orbit sizes (counted with multiplicities). Then we choose one point in each of $\Omega_1, \dots, \Omega_{d_1}$, and let G_2 act transitively on this set. The next domain of transitivity consists of a second point in Ω_{d_1} together with one point in each of $\Omega_{d_1+1}, \dots, \Omega_{d_1+d_2-1}$. We continue in this way, until either all m domains of transitivity are chosen, or all the Ω_i are linked. In the latter case we construct orbits of G_2 by taking one point not yet used which is moved by G_1, and add sufficiently many fixed points of G_1 to obtain a domain of transitivity for G_2 of the required size. In this way we continue until one of the following happens: all orbits of G_2 are chosen, there are not sufficient fixed points of G_1 left to choose from, or all points moved by G_1 are used up, but there are still orbits for G_2 to be constructed. In the first case, we have constructed an action of G_2 such that the number of orbits is in fact as small as predicted, whereas in the second case we construct one orbit of G_2 consisting of the remaining points fixed by G_1, and arbitrary other points not yet used for G_2, thereby reaching a transitive action. In the last case, all points moved by G_1 are also moved by G_2, but there is at least one orbit of G_2 of size ≥ 2 containing only 1 point moved by G_1, that is, G_2 has less fixed points then G_1, contrary to our choice of G_1. Hence, the last case cannot happen. Now we repeat this argument for the groups $G_3, \dots, G_s$: let $\Omega'_1, \dots, \Omega'_{\ell'}$ be the domains of transitivity of $\langle G_1, G_2\rangle$, and choose the domains of G_3 with respect to these sets. Again, we either obtain a transitive action, or the number of orbits decreases by the right amount. We continue until the actions for all groups are defined, and either obtain a transitive action at some intermediate stage, or reach it in the final step. Hence, we obtain a transitive action determining a group Δ with isomorphism type $\mathbf{t}$; that is, $\mathbf{t}$ is realized. □

At first sight, the second condition of Theorem 4 appears to be unwieldy; however, in every concrete situation, this condition can be given a transparent form. In fact, the non-zero entries of the tuple $(\nu_{\tau\sigma})$ are restricted by linear inequalities, and the possible values for (λ_τ) are the image of the occurring $(\nu_{\tau\sigma})$ under a linear map, hence, the second condition describes the lattice points in a certain polytope. Indeed, in the following example the occurrence of the modulus 7 appears more surprising than the inequalities.

Example 1. *Let $\Gamma = (C_2 \times C_2) * S_3$. Then there exists a finite-index subgroup Δ isomorphic to $C_2^{*\lambda_1} * C_3^{*\lambda_2} * (C_2 \times C_2)^{*\lambda_3} * S_3^{*\lambda_4} * F_\mu$ if, and only if,*

$$6\lambda_1 + 8\lambda_2 + 9\lambda_3 + 10\lambda_4 + 12\mu \equiv 5 \pmod 7$$

and the following inequalities are satisfied:

$$\begin{aligned} \lambda_1, \lambda_2, \lambda_3, \lambda_4, \mu &\geq 0, \\ 5\lambda_1 + 2\lambda_2 + \lambda_3 + \lambda_4 &\leq 2n, \\ \lambda_3 &\leq n, \\ 2\lambda_2 + \lambda_4 &\leq n, \end{aligned}$$

with the exceptions of $\Delta = C_\infty$ *and* $\Delta = C_2 * C_2$, *which cannot occur as finite-index subgroups.*

Proof. Expanding Condition (i), we find that the quantity

$$\frac{6\lambda_1 + 8\lambda_2 + 9\lambda_3 + 10\lambda_4 + 12\mu - 12}{7}$$

has to be a positive integer. This expression is integral if, and only if, the stated congruence holds true, and it is non-positive only in the stated exceptional cases. Next, we have to consider the second condition of Theorem 4. In the notation of the theorem, we have $\nu_{21} = \nu_{32} = \nu_{42} = 0$, and the remaining five variables satisfy

$$\begin{aligned} \nu_{11}, \nu_{12}, \nu_{22}, \nu_{31}, \nu_{42} &\geq 0, \\ 2\nu_{11} + \nu_{31} &\leq n, \\ 3\nu_{12} + 2\nu_{22} + \nu_{42} &\leq n, \end{aligned}$$

as well as

$$\begin{aligned} \lambda_1 &= \nu_{11} + \nu_{12}, & \lambda_2 &= \nu_{22}, \\ \lambda_3 &= \nu_{13}, & \lambda_4 &= \nu_{42}. \end{aligned}$$

The last equations transform the stated inequalities for the $\nu_{\tau\sigma}$ into the stated inequalities for the λ_τ. □

The second condition in Theorem 4 becomes particularly simple, if for all $1 \leq \sigma_1, \sigma_2 \leq s$ the groups G_{σ_1} and G_{σ_2} are either isomorphic or have coprime order. In this case the resulting inequalities take the form

$$\sum_{\substack{\tau \\ (|U_\tau|, |G_\sigma|) > 1}} \frac{|G_\sigma|}{|U_\tau|} \lambda_\tau \leq n \sum_{\substack{\tau \\ (|U_\tau|, |G_\sigma|) > 1}} 1, \qquad (1 \leq \tau \leq t).$$

We next consider some miscellaneous applications of Theorem 1. Our first result deals with normal subgroups.

Proposition 4. *Let* Γ *be as in* (1), *and let* Δ *be a normal subgroup of index* n *in* Γ *and with isomorphism type* $(\lambda_1, \dots, \lambda_t; \mu)$. *Then* $n \mid \lambda_\tau m_\tau$ *for all* τ, *where* m_τ *is the least common multiple of* $\frac{|G_\sigma|}{|U_\tau|}$ *taken over all* σ *such that* U_τ *is isomorphic to a subgroup of* G_σ.

Proof. If Δ is normal in Γ, the restriction of the corresponding permutation representation to G_σ is similar to a multiple of some transitive representation; hence, $m_{\sigma\kappa}$ is either 0 or $\frac{n}{d_{\sigma\kappa}}$. Our claim now follows from Theorem 1. □

Corollary 1. *Let Γ be as in* (1), *and let m_Γ be the least common multiple of $|G_1|, \dots, |G_\sigma|$. Then for a subgroup Δ of index n with isomorphism type $(\lambda_1, \dots, \lambda_t; \mu)$ the index $(N_\Gamma(\Delta) : \Delta)$ divides each entry of the tuple $(n, m_\Gamma\lambda_1, \dots, m_\Gamma\lambda_t)$.*

Proof. Apply Proposition 4 to $N_\Gamma(\Delta)$ instead of Γ and note that each m_τ is a divisor of m_Γ. □

Corollary 2. *Let G_1, G_2 be finite groups, G_1 not isomorphic to a subgroup of G_2, and let Δ be a normal subgroup of $\Gamma = G_1 * G_2$ which has G_1 as free factor. Then Γ/Δ is a quotient of G_2.*

Proof. By Theorem 1 we know that G_1 is a free factor of Δ if and only if the action of G_1 on Δ has at least one fixed point. If Δ is normal, this implies that the action of G_1 is trivial, hence, the map $\Gamma \to G_1 * G_2$ factors through G_2, which implies our claim. □

Corollary 3. *Let $\bar{f}(n)$ be the number of normal subgroups of index n in $\Gamma = C_2 * C_4$ which are not free. Then we have $\bar{f}(n) = 1$ for even n, and $\bar{f}(n) = 0$ for odd n with the exceptions $\bar{f}(1) = 1$, $\bar{f}(2) = 3$, and $\bar{f}(4) = 2$.*

Proof. Checking the groups of order ≤ 4 individually, it suffices to prove our claim for $n \geq 5$. Let Δ be a normal subgroup of index n which is not free, and let x, y be generators of Γ such that $x^2 = y^4 = 1$. If one of x and y acts trivially on Γ/Δ, we would have $n \leq 4$, if both would act regularly, Δ would be free. Hence, we may suppose that both x and y act by 2-cycles only, so that the map $\Gamma \to \Gamma/\Delta$ factors through $\Gamma/\langle\!\langle y^2 \rangle\!\rangle$, which is isomorphic to $C_2 * C_2$. On the other hand, each free normal subgroup of $C_2 * C_2$ defines a regular action of x and y^2, thus a non-free normal subgroup of Γ. Hence, for $n \geq 5$ the number of non-free normal subgroups of Γ equals the number of free normal subgroups of $C_2 * C_2$, which is 1 for even $n \geq 6$ and 0 for n odd. □

Next we show that a slight sharpening of the conditions of Theorem 4 ensures existence of non-maximal subgroups of given type. This observation is remarkable, since in the context of large groups usually almost all subgroups are maximal; cf. Proposition 6 for the case of groups of the form (1).

Proposition 5. *Let Γ be as in* (1), *and suppose that $\chi(\Gamma) < 0$. Then there exists some constant c such that the following holds true. Let $\mathbf{t} = (\lambda_1, \dots, \lambda_t; \mu)$ be a tuple of non-negative integers satisfying Condition* (i) *in Theorem 4. Suppose there exist integers $\nu_{\tau\sigma}$ such that $\nu_{\tau\sigma} = 0$ for all τ with the property that G_σ does not contain a subgroup isomorphic to U_τ, $\sum_\sigma \nu_{\tau\sigma} = \lambda_\tau$ and*

$$\sum_\tau \nu_{\tau\sigma} \leq \alpha n - c \min_{d|n}(d + n/d),$$

where $\alpha = \min\left(1, \frac{-\chi(\Gamma)}{-\chi(\Gamma) - r + 1}\right)$. Then there exists a non-maximal subgroup Δ of finite index in Γ, which is of type $\mathbf{t}$.

Proof. Our assertion holds trivially if Γ is free, so suppose that Γ is not free. Let d be a divisor of n. We first choose a subgroup Δ' of index d which is close to being a free power of Γ, that is, if we order the groups $U_1, \dots, U_t$ in such a way that

$\{U_1, \dots, U_r\} = \{G_1, \dots, G_s\}$ we look for a subgroup Δ' of index d with isomorphism type $\mathbf{t}' = (m_1 x, m_2 x, \dots, m_r x, 0, \dots, 0; \mu)$ where m_τ is the number of groups among $G_1, \dots, G_s$, which are isomorphic to U_τ, and μ is as small as possible. Altering x by a bounded amount, we can always ensure integrality of the quotient corresponding to Δ' occurring in Condition (i) of Theorem 4. The inequalities in Condition (ii) become fairly easy due to the special structure of $\mathbf{t}'$. In fact, choosing the $\nu_{\tau\sigma}$ in such a way that $\nu_{\tau\sigma} = 0$ unless $G_\sigma \cong U_\tau$, we obtain the inequalities $m_\tau x \leq m_\tau d$, that is the second condition is satisfied for $x \leq d$. The Euler characteristic equation yields

$$\sum_{\tau=1}^{r} m_\tau x\big(1 - \frac{1}{|U_\tau|}\big) + \mu - 1 = d\Big(\sum_{\tau=1}^{r} m_\tau\big(1 - \frac{1}{|U_\tau|}\big) + r - 1\Big),$$

which is compatible with the condition $\mu \geq 0$ provided that

$$x \leq d\frac{\sum_{\tau=1}^{r} m_\tau\big(1 - \frac{1}{|U_\tau|}\big) + r - 1}{\sum_{\tau=1}^{r} m_\tau\big(1 - \frac{1}{|U_\tau|}\big)} = d\frac{-\chi(\Gamma)}{-\chi(\Gamma) + 1 - r},$$

where the last quotient is positive since $\chi(\Gamma) < 0$ and Γ is not free. Combining these estimates, we find that there exists a subgroup Δ' of index d and type $\mathbf{t}'$ with $x > \alpha d - C_1$ for some C_1 depending only on Γ and α as in the proposition. Next, we have to show that Δ' has a subgroup of index n/d with type $\mathbf{t}$. To do so, we take $\Gamma = \Delta'$ in Theorem 4. By assumption, $\mathbf{t}$ satisfies Condition (i) with respect to Γ, hence, by multiplicativity of the Euler characteristic, $\mathbf{t}$ satisfies this condition with respect to Δ' as well, and it suffices to find integers $\nu'_{\tau\sigma}$ satisfying Condition (ii) with respect to Δ'. Since every finite free factor of Γ occurs x-times as free factor of Δ', our task is to find non-negative integers $\nu'_{\tau\sigma k}$ for $1 \leq \tau \leq t$, $1 \leq \sigma \leq s$, and $1 \leq k \leq x$ such that $\nu'_{\tau\sigma k} = 0$ unless U_τ is isomorphic to a subgroup of G_σ, $\sum_{\sigma,k} \nu'_{\tau\sigma k} = \lambda_\tau$ and $\sum_\tau \nu'_{\tau\sigma k} \leq n/d$. We do so by choosing $\nu'_{\tau\sigma k} \in \{[\nu_{\tau\sigma}/x], [\nu_{\tau\sigma}/x] + 1\}$ such that $\sum_k \nu'_{\tau\sigma k} = \nu_{\tau\sigma}$. Clearly, $\nu'_{\tau\sigma k} = 0$ whenever $\nu_{\tau\sigma} = 0$, and the integers $\nu'_{\tau\sigma k}$ induce the isomorphism type $\mathbf{t}$. It remains to check that $\sum_\tau \nu'_{\tau\sigma k} \leq n/d$. We have

$$\begin{aligned}\sum_\tau \nu'_{\tau\sigma k} \; &\leq \; \sum_\tau \Big[\frac{\nu_{\tau\sigma}}{x}\Big] + 1 \; \leq \; \frac{1}{x}\sum_\tau \nu_{\tau\sigma} + t \\ &\leq \; \frac{1}{\alpha d - C_1}\sum_\tau \nu_{\tau\sigma} + t \; \leq \; \frac{1}{\alpha d}\sum_\tau \nu_{\tau\sigma} + t + C_2\frac{n}{d^2} \; \leq \frac{n}{d},\end{aligned}$$

provided that $\sum_\tau \nu_{\tau\sigma} \leq \alpha n - C_3(d + n/d)$. □

As we shall see later, almost all subgroups of index n have type $(\lambda_1, \dots, \lambda_t; \mu)$ with $\lambda_\tau \ll \sqrt{n}$, thus even for $\alpha < 1$ the conditions of Proposition 5 are satisfied for almost all subgroups; that is, almost all subgroups of finite index have an isomorphism type realized by a non-maximal finite-index subgroup.

4. Asymptotic enumeration of isomorphism types

For a representation type $\mathbf{m} = (m_{\sigma\kappa})_{\substack{1\leq\sigma\leq s\\ 1\leq\kappa\leq k_\sigma}}$ denote by $s_{\mathbf{m}}(\Gamma)$ the number of subgroups Δ with representation type $\mathbf{m}$. Note that the representation type determines the index, hence, $s_{\mathbf{m}}$ is finite for all $\mathbf{m}$. Similarly, for an isomorphism type $\mathbf{t}$ denote by $s_{\mathbf{t}}$ the number of finite-index subgroups realizing $\mathbf{t}$. We will now give an asymptotic formula for $s_{\mathbf{m}}$ for a certain domain of representation types.

Theorem 5. *Let Γ be as in (1), let p_σ be the least prime divisor of $|G_\sigma|$, and let $\varepsilon > 0$ be given. Set*

$$\mathcal{M} = \Big\{(\ell_1, \dots, \ell_s) \in [0,1]^s : \sum_\sigma \min\big(\frac{p_\sigma - 1}{p_\sigma}, 1 - \ell_\sigma\big) > 1 + \varepsilon\Big\}.$$

Number the representations of the groups G_σ in such a way that $\rho_{\sigma 1}$ is the trivial representation for each σ. Then the asymptotic formula

$$s_{\mathbf{m}}(\Gamma) = \Big(1 + \mathcal{O}\big(n^{-\alpha+\varepsilon}\big)\Big)\frac{n \cdot n!^{s+r-1}}{\prod_{\sigma=1}^s \prod_{\kappa=1}^{k_\sigma} m_{\sigma\kappa}!\, d_{\sigma\kappa}^{m_{\sigma\kappa}}} \tag{9}$$

holds true with $\alpha = \sum_\sigma \min(\frac{p_\sigma-1}{p_\sigma}, 1 - \ell_\sigma) - 1$ uniformly in the set of all types $\mathbf{m}$ with the property that $(\frac{\log m_{11}}{\log n}, \dots, \frac{\log m_{s1}}{\log n}) \in \mathcal{M}$.

Our result is optimal in the sense that if in the definition of $\mathcal{M}$ we replace ε by $-\varepsilon$ the conclusion is false; however, (9) holds true e.g. for representation types containing many trivial and many very large orbits, which are not covered by the theorem. Comparing with Theorem 3, we find that Theorem 5 covers almost all subgroups, therefore we do not see much merit in aiming for the utmost generality.

Proof. Without loss we may assume that $\ell_\sigma \geq 1 - \frac{1}{p_\sigma}$ holds true for all σ. For a representation type $\mathbf{m}$ denote by $h_{\mathbf{m}}(\Gamma)$ the number of permutation representations of Γ of type $\mathbf{m}$, and by $h_{\mathbf{m}}^t(\Gamma)$ the number of transitive representations of type m. We have

$$h_{\mathbf{m}}(\Gamma) = \frac{n!^{s+r}}{\prod_{\sigma=1}^s \prod_{\kappa=1}^{k_\sigma} m_{\sigma\kappa}!\, d_{\sigma\kappa}^{m_{\sigma\kappa}}}$$

and

$$s_{\mathbf{m}}(\Gamma) = \frac{h_{\mathbf{m}}^t(\Gamma)}{(n-1)!};$$

hence, it suffices to show that the proportion of non-transitive representations among all permutation representations of type $\mathbf{m}$ is sufficiently small. We do so by bounding the probability that a random representation leaves invariant some proper subset Ω of $\{1, \dots, n\}$. Let ρ be a representation of type $\mathbf{m}$ chosen at random, and, for $1 \leq \sigma \leq s$, denote by $\rho^{(\sigma)}$ the induced representation of G_σ. Let Ω be an arbitrary set of size k, let P_k be the probability that $\rho^{(1)}$ stabilizes Ω, that is, the probability that Ω is the union of orbits of $\rho^{(1)}$, and let P_k^* be the conditional probability subject to the condition that $\rho^{(1)}$ acts without fixed points on Ω. We may suppose that $k \leq n/2$, since the complement of an invariant set is automatically invariant as well. By choosing fixed points first, we find that

$$P_k \leq \sum_{\nu=0}^k \binom{k}{\nu}\Big(\frac{m_{11}}{n}\Big)^\nu P_{k-\nu}^* \leq \sum_{\nu=0}^k \binom{k}{\nu} n^{-\nu(1-\ell_1)} P_{k-\nu}^*.$$

To estimate P_k^*, consider the orbit containing some point $a \in \Omega$. We know that this orbit has size $\geq p_\sigma$, the precise probability distribution of its orbit size being given by the distribution of orbit lengths of $\rho^{(1)}$.[1] Suppose that with probability Q_ℓ, $p_1 \leq \ell \leq |G_1|$, the orbit of 1 under $\rho^{(1)}$ consists of ℓ points. Then we have

$$P_k^* = \sum_{\ell=p-1}^{|G_1|} \binom{k-1}{\ell-1}\binom{n-1}{\ell-1}^{-1} Q_\ell P_{k-\ell}^* \leq \sum_{\ell=p-1}^{|G_1|} \Big(\frac{k-1}{n-1}\Big)^{\ell-1} Q_\ell P_{k-\ell}^*,$$

from which it follows by induction on k, using the fact that $\sum_\ell Q_\ell = 1$, that

$$P_k^* \leq k^{p_1}\Big(\frac{k!}{n^k}\Big)^{1-\frac{1}{p_1}},$$

and therefore

$$\begin{aligned} P_k &\leq k^{p_1}\sum_{\nu=0}^{k}\binom{k}{\nu} n^{-\nu(1-\ell_1)}\Big(\frac{(k-\nu)!}{n^{k-\nu}}\Big)^{1-\frac{1}{p_1}} \\ &\leq k^{c\sqrt{k}}\binom{n}{k}^{\ell_1-1}. \end{aligned}$$

Since there are $\binom{n}{k}$ sets Ω to consider, and the events '$\rho^{(\sigma)}$ fixes Ω' are stochastically independent, we find that the probability that there exists a set of k points left invariant by ρ is bounded above by

$$k^{c\sqrt{k}}\binom{n}{k}^{1-s+\sum_\sigma \ell_\sigma} \leq \binom{n}{k}^{1-s+\sum_\sigma \ell_\sigma+\varepsilon}$$

for $k \leq n/2$. Obviously,

$$\sum_{k=1}^{n/2}\binom{n}{k}^{1-s+\sum_\sigma \ell_\sigma+\varepsilon} \ll n^{1-s+\sum_\sigma \ell_\sigma+\varepsilon},$$

provided the exponent is negative, and our claim follows. □

As an illustration of the fact that more specific information on the representation type may be turned into a more precise asymptotic estimate, we note the following consequence of the argument leading to Theorem 5.[2]

Corollary 4. *Let Γ be as in* (1), *suppose that $\chi(\Gamma) < 0$, and denote by $f_n(\Gamma) = s_{(0,\dots,0;\mu)}(\Gamma)$ the number of free subgroups of index n in Γ, where $\mu = -n\chi(\Gamma)+1$. Then we have for any fixed $\varepsilon > 0$ the estimate*

$$f_n(\Gamma) = \Big(1+\mathcal{O}\big(n^{\chi(\Gamma)+\varepsilon}\big)\Big)\prod_{\sigma=1}^{s}\frac{n!}{(n/|G_\sigma|)!|G_\sigma|^{n/|G_\sigma|}},$$

if n is divisible by $|G_\sigma|$ for all σ, and $f_n(\Gamma) = 0$ otherwise.

We are now in a position to prove Theorem 2.

[1] It is at this point that one can obtain better results provided more detailed information on $\mathbf{m}$ is available.

[2] A more precise result for the free subgroup growth of an arbitrary virtually free group can be found in [9].

Proof of Theorem 2. In view of Theorem 1 we have for an isomorphism type $\mathbf{t} = (\lambda_1, \dots, \lambda_t; \mu)$ the equation

$$s_{\mathbf{t}}(\Gamma) = \sum_{\substack{\mathbf{m}=(m_{\sigma\kappa})\\ \forall\tau: \sum\limits_{\sigma,\kappa:\mathrm{Stab}_{\rho_{\sigma\kappa}}(1)\cong U_\tau} m_{\sigma\kappa}=\lambda_\tau}} s_{\mathbf{m}}(\Gamma).$$

By assumption, the number of fixed points of all occurring representations is sufficiently small to apply Theorem 5, and by collecting all terms which do not depend on $\mathbf{m}$ we obtain

$$\begin{aligned} s_{\mathbf{t}}(\Gamma) &= \Big(1+\mathcal{O}\big(n^{-\alpha+\varepsilon}\big)\Big)\sum_{\mathbf{m}} \frac{n\cdot n!^{s+r-1}}{\prod_{\sigma=1}^{s}\prod_{\kappa=1}^{k_\sigma} m_{\sigma\kappa}!\, d_{\sigma\kappa}^{m_{\sigma\kappa}}}\\ &= \Big(1+\mathcal{O}\big(n^{-\alpha+\varepsilon}\big)\Big)\frac{n\cdot n!^{s+r-1}}{\prod_{\tau=1}^{t}|U_\tau|^{\lambda_\tau}}\sum_{\mathbf{m}}\frac{1}{\prod_{\sigma=1}^{s}\prod_{\kappa=1}^{k_\sigma} m_{\sigma\kappa}!}. \qquad (10)\end{aligned}$$

We compute the right-hand side of the last equation by means of the generating function

$$F(z_1,\dots,z_t) = \sum_{n_1,\dots,n_t\geq 0} z_1^{n_1}\cdots z_t^{n_t} \sum_{\substack{\rho=(m_{\sigma\kappa})\\ \forall\tau: \sum\limits_{\sigma,\kappa:\mathrm{Stab}_{\rho_{\sigma\kappa}}(1)=U_\tau} m_{\sigma\kappa}=n_\tau}} \frac{1}{\prod_{\sigma=1}^{s}\prod_{\kappa=1}^{k_\sigma} m_{\sigma\kappa}!}.$$

For σ, κ define $\tau(\sigma,\kappa)$ to be the unique index τ such that $\mathrm{Stab}_{\rho_{\sigma\kappa}}(1) \cong U_\tau$. Then we have

$$\begin{aligned} F(z_1,\dots,z_t) &= \prod_{\sigma=1}^{s}\prod_{\kappa=1}^{k_\sigma}\sum_{m_{\sigma\kappa}\geq 0}\frac{z_{\tau(\sigma,\kappa)}^{m_{\sigma\kappa}}}{m_{\sigma\kappa}!}\\ &= \prod_{i=\tau}^{t}\exp(\mu_\tau z_\tau)\\ &= \sum_{n_1,\dots,n_t}\frac{\mu_1^{n_1}\cdots\mu_t^{n_t}}{n_1!\cdots n_t!} z_1^{n_1}\cdots z_t^{n_t}.\end{aligned}$$

Inserting the coefficient of $z_1^{\lambda_1}\cdots z_t^{\lambda_t}$ into (10) yields our claim. □

Proposition 6. *Let* Γ *be as in* (1), *and suppose that* $\chi(\Gamma) < 0$. *Denote by* $s_n^{\neg\max}(\Gamma)$ *the number of non-maximal subgroups of index* n *in* Γ. *Then we have for any fixed* $\varepsilon > 0$ *the estimate*

$$\frac{s_n^{\neg\max}(\Gamma)}{s_n(\Gamma)} \ll 2^{(\chi(\Gamma)+\varepsilon)n},$$

in particular, almost all finite-index subgroups are maximal.

Proof. The proof runs parallel to that of [12, Prop. 9], therefore, we only sketch the argument. Define $h_n^{t,\neg\max}(\Gamma)$ to be the number of homomorphisms $\varphi : \Gamma \to S_n$ such that $\varphi(\Gamma)$ acts transitively and imprimitively on $[n]$. We have $s_n^{\neg\max}(\Gamma) = h_n^{t,\neg\max}(\Gamma)/(n-1)!$ as well as $h_n^t \sim h_n$, hence, it suffices to bound $h_n^{t,\neg\max}(\Gamma)/h_n$. Let φ be a homomorphism counted by $h_n^{t,\neg\max}(\Gamma)$, Ω a domain of imprimitivity for φ consisting of d points.

The image of $\varphi(\Gamma)$ is contained in a subgroup of S_n isomorphic to $S_d \wr S_{n/d}$, which is determined by Ω and its translates. Hence, we obtain the inequality

$$h_n^{t,\neg\max}(\Gamma) \leq \sum_{\substack{d|n\\1<d<n}} (n/d)!^{-1}\binom{n}{d,\dots,d}|S_d \wr S_{n/d}|^r \prod_{\sigma=1}^{s} |\operatorname{Hom}(G_\sigma, S_d \wr S_{n/d})|. \tag{11}$$

For $\tau = 1,\dots,t$ define functions

$$f_\tau(n) = \left(\frac{|\operatorname{Hom}(U_\tau, S_n)|}{n!^{1-1/|U_\tau|}}\right)^{1/n}$$

and $f(n) = \max_\tau f_\tau(n)$. Setting $H = \{1\}$ in the first part of Lemma 1 we obtain

$$|\operatorname{Hom}(U_\tau, S_n)| = n!^{1-1/|U_\tau|}e^{\mathcal{O}(\sqrt{n})},$$

and therefore that f is bounded and tends to 1 as $n \to \infty$. To evaluate $|\operatorname{Hom}(G_\sigma, S_d \wr S_{n/d})|$, first choose a homomorphism $\psi : U_\tau \to S_{n/d}$ of representation type $\mathbf{m} = (m'_\kappa)_{1\leq\kappa\leq k_\tau}$. Then the number of extensions of a given ψ to a homomorphism $G_\sigma \to S_d \wr S_{n/d}$ equals

$$d!^{n/d-\sum m'_\kappa}\prod_{\kappa=1}^{k_\tau}|\operatorname{Hom}(U_\tau, S_d)|^{m'_\kappa},$$

where U_τ is the stabilizer of the representation $\rho_{\sigma\kappa}$ of G_σ. Hence we obtain

$$\begin{aligned}|\operatorname{Hom}(G_\sigma, S_d \wr S_{n/d})| = \sum_{\mathbf{m}} d!^{n/d-\sum m'_\kappa}\prod_{\kappa=1}^{k_\tau}|\operatorname{Hom}(U_\tau, S_d)|^{m'_\kappa}&\\ \times\left|\left\{\psi : G_\sigma \to S_{n/d} : \psi \text{ realizes } \mathbf{m}\right\}\right|,&\end{aligned}$$

where the summation runs over all representation types $\mathbf{m} = (m'_\kappa)$ of U_τ in S_d. We now simplify the right-hand expression by introducing f and use the fact that $\sum_\kappa m'_\kappa \frac{|G_\sigma|}{|U_\kappa|} = \frac{n}{d}$, to obtain

$$\begin{aligned}|\operatorname{Hom}(G_\sigma, S_d \wr S_{n/d})| &\leq d!^{n/d}\sum_{\mathbf{m}}\prod_{\kappa=1}^{k_\tau}\left(\frac{f(d)\,d!^{1-1/|U_\kappa|}}{d!}\right)^{m'_\kappa}\\ &\qquad\times\left|\left\{\psi : G_\sigma \to S_{n/d} : \psi \text{ realizes } \mathbf{m}\right\}\right|\\ &\leq d!^{(1-1/|G_\sigma|)n/d}f(d)^{n/d}\sum_{\mathbf{m}}\left|\left\{\psi : G_\sigma \to S_{n/d} : \psi \text{ realizes } \mathbf{m}\right\}\right|\\ &= d!^{(1-1/|G_\sigma|)n/d}f(d)^{n/d}|\operatorname{Hom}(G_\sigma, S_{n/d})|\\ &\leq d!^{(1-1/|G_\sigma|)n/d}f(d)^{n/d}f(n/d)^{n/d}(n/d)!^{1-1/|G_\sigma|}.\end{aligned}$$

Inserting this bound into (11) and arguing as in [12, section 6.2, pp. 35–36] our claim follows. □

5. Distribution of isomorphism types

Lemma 3. *Let G be a finite group of order m. Then there exist constants c_d, $d|m$, such that*
$$\frac{|\operatorname{Hom}(G,S_n)|}{|\operatorname{Hom}(G,S_{n-\ell})|} = n^{\ell(1-1/m)}\Big(1+\ell\sum_{\substack{d|m\\ d<m}} c_d n^{-1+d/m} + \mathcal{O}\Big(\frac{\ell^2}{n}\Big)\Big)$$
uniformly in $\ell < \sqrt{n}$.

Proof. For $\ell = 1$ this follows from [10, Theorem 6]. We now write
$$\frac{|\operatorname{Hom}(G,S_n)|}{|\operatorname{Hom}(G,S_{n-\ell})|} = \prod_{\nu=n-\ell+1}^{n} \nu^{(1-1/m)}\Big(1+\sum_{\substack{d|m\\ d<m}} c_d \nu^{-1+d/m} + \mathcal{O}\Big(\frac{1}{n}\Big)\Big)$$
and consider the two factors separately. The first factor yields
$$\begin{aligned}\prod_{\nu=n-\ell+1}^{n} \nu^{(1-1/m)} &= n^{\ell(1-1/m)} \exp\Big(-(1-1/m)\sum_{\nu=n-\ell+1}^{n}\frac{n-\nu}{n} + \mathcal{O}\Big(\frac{\ell^2}{n^2}\Big)\Big)\\ &= n^{\ell(1-1/m)}\Big(1+\mathcal{O}\Big(\frac{\ell^2}{n}\Big)\Big),\end{aligned}$$
whereas the second factor can be written as
$$\exp\Big(\sum_{\nu=n-\ell+1}^{n}\log\Big(1+\sum_{\substack{d|m\\ d<m}} c_d\nu^{-1+d/m}+\mathcal{O}\Big(\frac{1}{n}\Big)\Big)\Big) = \exp\Big(\sum_{\nu=n-\ell+1}^{n}\sum_{\substack{d|m\\ d<m}} c_d\nu^{-1+d/m}+\mathcal{O}\Big(\frac{1}{n}\Big)\Big),$$
where we have inserted the Taylor series for $\log(1+z)$. Note that the largest occurring exponent of ν is $\leq -1/2$, hence, in the Taylor series for $\log(1+z)$ all terms of order higher than linear can be absorbed into the error term. Since $n^{-1+d/m} - \nu^{-1+d/m} \ll \ell n^{-2+d/m}$, we obtain
$$\begin{aligned}\prod_{\nu=n-\ell+1}^{n}\Big(1+\sum_{\substack{d|m\\ d<m}} c_d\nu^{-1+d/m}+\mathcal{O}\Big(\frac{1}{n}\Big)\Big) &= \exp\Big(\ell\sum_{\substack{d|m\\ d<m}} c_d n^{-1+d/m} + \mathcal{O}\Big(\frac{\ell}{n}+\frac{\ell^2}{n^{3/2}}\Big)\Big)\\ &= 1+\ell\sum_{\substack{d|m\\ d<m}} c_d n^{-1+d/m} + \mathcal{O}\Big(\frac{\ell^2}{n}\Big),\end{aligned}$$
where we have again used the fact that n appears with exponent $-1/2$ at most. Our claim now follows by combining the preceding estimates. □

Lemma 4. *Let G be a finite group of order m, and let $\rho_1,\dots,\rho_k$ be a complete list of non-regular transitive permutation representations of G, where ρ_i acts on m_i points, and let ρ be the regular representation. Define random variables $\xi_i^{(n)}$, $1 \leq i \leq k$, as follows. Let $\varphi : G \to S_n$ be a permutation representation chosen at random, and set $\varphi = \kappa\rho \oplus \bigoplus \xi_i^{(n)}\rho_i$. Then, as $n \to \infty$, the $\xi_i^{(n)}$ are asymptotically independent, and $\frac{\xi_i^{(n)} - n^{m_i/m}}{n^{m_i/2m}}$ converges to a standard normal distribution. More precisely, denote by*

$M_r^{(n)}$ the r-th moment of $\xi_i^{(n)}$, and by $\tilde{M}_r$ the r-th moment of the corresponding normal distribution. Then we have

$$M_r^{(n)} = \big(1 + \mathcal{O}(r^2 n^{-1/m_i})\big)\tilde{M}_r \tag{12}$$

uniformly in $r < \sqrt{n}$.

Proof. For $\varphi : G \to S_n$ chosen at random, define for $1 \leq i \leq n$ the random variable ζ_i to be k, if G acts on the orbit of i as described by ρ_k, and $\zeta_i = 0$, if G acts regularly on the orbit of ρ_i. We first compute the probability of the event $\zeta_1 = k$. Every homomorphism $\varphi : G \to S_n$ such that G acts on the orbit of 1 like ρ_k can be constructed as follows. First, choose the orbit of 1, which can be done in $\binom{n-1}{m_k-1}$ ways; then identify the points in the orbit with cosets of the stabilizer of 1, which can be done in $(m_k - 1)!$ ways. Finally, on the remaining $n - m_k$ points, choose an arbitrary action of G. Hence, using Lemma 3, we obtain

$$\begin{aligned} P(\zeta_1 = k) &= \frac{n(n-1)\cdots(n-m_k+2)|\operatorname{Hom}(G, S_{n-m_k})|}{\operatorname{Hom}(G, S_n)} \\ &= n^{\frac{m_k}{|G|}-1}\left\{1 + \sum_{\nu=1}^{m-1} c_\nu n^{-\nu/m} + \mathcal{O}(n^{-1})\right\}. \end{aligned}$$

Next we compute the probability of the event $\zeta_1 = k$ under the condition that $\zeta_2 = a_2, \dots, \zeta_r = a_r$. First choose the orbits containing $2, \dots, r$. With probability $1 + \mathcal{O}(rn^{-1})$, the point 1 is not contained in the union of these orbits; that is, the probability for $\zeta_1 = k$ is the same as the probability for a randomly chosen representation $G \to S_{n-\ell}$, where ℓ denotes the size of the union of the orbits of $2, \dots, r$. Hence, we obtain

$$\begin{aligned} &P(\zeta_1 = k \,|\, \zeta_2 = a_2, \dots, \zeta_r = a_r) \\ &\qquad = \frac{(n-\ell)\cdots(n-\ell-m_k+2)|\operatorname{Hom}(G, S_{n-\ell-m_k})|}{|\operatorname{Hom}(G, S_{n-\ell}|)} + \mathcal{O}(rn^{-1}). \end{aligned}$$

Inserting Lemma 3, we obtain

$$P(\zeta_1 = k \,|\, \zeta_2 = a_2, \dots, \zeta_r = a_r) = P(\zeta_1 = k)\big(1 + \mathcal{O}(r^2 n^{-1})\big) + \mathcal{O}(rn^{-1});$$

hence, the variables $\xi_k^{(n)}$ are asymptotically independent. Set $\eta_i = 1$ if $\zeta_i = k$, and $\eta_i = 0$ otherwise, and let $\hat{\eta}_i$ be independent random variables with the same distribution. Then we obtain

$$\begin{aligned} \mathbf{E}\left(\sum_{i=1}^n \eta_i\right)^r - \mathbf{E}\left(\sum_{i=1}^n \hat{\eta}_i\right)^r &= \sum_{\substack{I\subseteq[n]\\|I|=r}} \mathbf{E}\big(\prod_{i\in I}\eta_i\big) - \prod_{i\in I}\mathbf{E}\eta_i \\ &= \binom{n}{r}\left(\prod_{i=1}^r P(\eta_i = 1 \,|\, \eta_1 = \dots = \eta_{i-1} = 1) - P(\eta_1 = 1)^r\right) \\ &\ll \binom{n}{r} P(\eta_1 = 1)^r \left(\frac{r^3}{n^2} + \frac{r^2}{nP(\eta_1 = 1)}\right) \\ &\ll \mathbf{E}\left(\sum_{i=1}^n \hat{\eta}_i\right)^r \left(\frac{r^3}{n^2} + \frac{r^2}{n^{1/m_k}}\right), \end{aligned}$$

which implies the claimed estimates for the moments of ξ_i. The convergence to a normal distribution now follows form the fact that the normal distribution is determined by its moments. □

We now use Theorem 1 together with Lemma 4 to prove Theorem 3.

Proof of Theorem 3. By Theorem 5 we know that almost all permutation representations ρ with $m_{\sigma\kappa} = o(n)$ are transitive, whereas from Lemma 4 we find that almost all subgroups have representation type satisfying $m_{\sigma\kappa} \ll \sqrt{n}$; moreover, in the range $r < \sqrt{n}$ other types occur too seldomly to influence the r-th moment significantly. Hence, instead of transitive representations it suffices to consider all permutation representations. The distribution of the representation type of a random homomorphism is given by Lemma 4, and by Theorem 1 this distribution is mapped onto a distribution of isomorphism types. All occurrences of U_τ as a subgroup of some G_σ such that $(G_\sigma : U_\tau) > d_\tau$ yield normal distributions with mean value $\ll n^{1/(d_\tau+1)}$, which are negligible, that is, up to an error of size $n^{1/d_\tau(d_\tau+1)}$, ξ_τ is the sum of m_τ independent random variables satisfying (12), and our claim follows from the fact that the sum of independent normally distributed variables is again normally distributed with parameters behaving additively. □

References

[1] The GAP Group, GAP – Groups, Algorithms, and Programming.

[2] GAP Reference manual, version 4.4.12, `www.gap-system.org/~gap/Manuals/doc/ref/manual.pdf`

[3] F. Klein and R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, Teubner, Leipzig, 1890 (Vol. 1) and 1892 (Vol. 2).

[4] F. Klein and R. Fricke, *Vorlesungen über die Theorie der automorphen Funktionen*, Teubner, Leipzig, 1897 (Vol. 1) and 1901 (Vol. 2).

[5] R. Kulkarni, A new proof and an extension of a theorem of Millington on the modular group, *Bull. London Math. Soc.* **17** (1985), 458–462.

[6] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, Birkhäuser, Basel, 2003.

[7] M. H. Millington, On cycloidal subgroups of the modular group, *Proc. London Math. Soc.* **19** (1969), 164–176.

[8] M. H. Millington, Subgroups of the classical modular group, *J. London Math. Soc.* **1** (1969), 351–357.

[9] T. Müller, Counting free subgroups of finite index, *Arch. Math.* **59** (1992), 525–532.

[10] T. Müller, Finite group actions and asymptotics of $e^{P(z)}$, *Combinatorica* **17** (1997), 523–554.

[11] T. Müller, Enumerating representations in finite wreath products, *Adv. Math.* **153** (2000), 118–154.

[12] T. W. Müller and J.-C. Schlage-Puchta, Classification and statistics of finite index subgroups in free products, *Adv. Math.* **188** (2004), 1–50.

[13] T. W. Müller and J.-C. Schlage-Puchta, Asymptotic stability for sets of polynomials, *Arch. Math. Brno* **41** (2005), 151–155.

[14] M. Newman, *Integral matrices*, Academic Press, 1972.

[15] H. Petersson, Über einen einfachen Typus von Untergruppen der Modulgruppe, *Archiv d. Math.* **4** (1953), 308–315.

[16] H. Petersson, Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe, *J. Reine u. Angew. Math.* **250** (1971), 182–212.

[17] H. Petersson, Konstruktionsprinzipien für Untergruppen der Modulgruppe mit einer oder zwei Spitzenklassen, *J. Reine u. Angew. Math.* **268/69** (1974), 94–109.

[18] D. Singerman, Subgroups of Fuchsian groups and finite permutation groups, *Bull. London Math. Soc.* **2** (1970), 319–323.

[19] W. W. Stothers, Impossible specifications for the modular group, *Manuscripta Math.* **13** (1974), 415–428.

Thomas W. Müller, School of Mathematical Sciences, Queen Mary & Westfield College, The University of London, Mile End Road, London E1 4NS, United Kingdom

Jan-Christoph Schlage-Puchta, Mathematisches Institut, Universität Freiburg, Eckerstr. 1, 79104 Freiburg, Germany
Current address: Department of pure mathematics and computer algebra, University of Ghent, Krijgslaan 281 S22, 9000 Ghent, Belgium