Matemática Contemporânea, Vol. 20, 227–272
http://doi.org/10.21711/231766362001/rmc204

FIVE LECTURES ON GENERALIZED PERMUTATION REPRESENTATIONS

Thomas Müller

The lectures recorded below are concerned with the theory of generalized permutation representations, which was conceived during my stay at the Mathematical Sciences Research Institute, Berkeley, California, in 1996/97 and further developed in 1997–98, with some work (related to the Poincaré–Klein problem) still ongoing. This fascinating theory, which is characterized by a fruitful interplay between group theory, combinatorics, and analysis, apart from its intrinsic interest, also has important applications in asymptotic group theory and the theory of Quillen complexes. The purpose of my lectures, which were delivered during the XVI. Escola de Álgebra (23 – 29 July 2000) at the University of Brasilia (UnB), was to outline, in as elementary and untechnical a fashion as possible, some of the major aspects of this theory, stressing motivation and background.

The first lecture recalls a more or less well known combinatorial aspect of permutation representations: given, say, a finitely generated group Γ, the problem of enumerating the permutation representations of Γ by degree, and that of counting finite index subgroups in Γ by index are related via a transformation, which, on the level of appropriate generating functions, takes the form of the logarithmic derivative (cf. Proposition 1). From a somewhat more philosophical point of view the existence of such a transformation formula means that enumerating permutation representations of a group Γ yields *decodable information* on structural invariants of Γ. It is this important observation which provides a first decisive hint towards our task. In dealing with possible generalizations of permutation representations we will have to start from some *class* $\mathcal{R}$ of sequences

$R_0, R_1, \ldots$ of finite groups, which is a fairly natural and technically sufficiently controlled 'neighbourhood' of the sequence $\{S_n\}$ of symmetric groups, and it is far from clear from the outset where to look for such a class. However, we will also have to exhibit a *criterion*, applicable to members $\{R_n\} \in \mathcal{R}$, when such a sequence is to be admitted as a proper generalization of permutation representations. Building on the above idea the criterion we are going to propose is that the generating function

$$\sum_{n\geq 0} |\mathrm{Hom}(\Gamma, R_n)|\, z^n/n!$$

can be decomposed in terms of the representation sequence $\{R_n\}$ and invariants of Γ *for all finitely generated groups* Γ. The task of specifying an appropriate class $\mathcal{R}$ of representation sequences which forms a natural and technically sufficiently controlled environment for pursuing the problem of generalizing permutation representations from this combinatorial point of view is taken up in the second lecture. The class $\mathcal{R}$ we are going to use consists of all sequences of the form

$$(H \wr \Pi_n)_N := \Big\{(f,\pi) \in H \wr \Pi_n : \; \prod_i f(i) \in N\Big\}, \quad n \geq 0,$$

where H is a finite group, $N \trianglelefteq H$ is a normal subgroup with H/N abelian, and $\{\Pi_n\}$ denotes the sequence $\{S_n\}$ of symmetric groups or the sequence $\{A_n\}$ of alternating groups. As it turns out, such a sequence satisfies the above criterion if and only if $(H : N) \leq 2$, and the main result of the second lecture, Theorem A, establishes (a somewhat refined version of) our criterion in the latter case. Lecture III, after discussing some special cases of Theorem A, culminates in an explicit formula (Theorem B) for computing the exterior function Φ_Γ, one of the key ingredients in our description of the generating functions

$$\sum_{n\geq 0} |\mathrm{Hom}(\Gamma, (H \wr \Pi_n)_N)|\, z^n/n!.$$

The last two lectures link the theory of generalized permutation representations to other important topics in group theory. In Lecture IV we explain how explicit formulae for elementary abelian groups supplied by our theory together with certain analytic considerations may be used to produce an efficient and extremely fast algorithm for computing the Euler characteristic of Quillen complexes associated with members of one of the representation sequences introduced above. The final lecture is concerned with explicit asymptotic estimates for the function $|\mathrm{Hom}(G, H \wr S_n)|$, where G and H are finite groups, and the connection of such estimates with the theory of subgroup growth. A famous problem, originally raised in the 1880's by Klein and Poincaré in connection with the construction of modular forms, asks (roughly speaking) for the asymptotic distribution of the isomorphism types of subgroups in the modular group and other free products. Lecture V concludes with some remarks concerning the latter problem and describes the impact of the results explained in the earlier parts of that lecture towards its solution.

It is my pleasure to thank Professor Said Sidki and the other members of the Scientific Committee for inviting these lectures, and the Mathematics Department of UnB for its warm hospitality. Thanks are also due to the Royal Society for supporting my participation through a conference travel grant.

The First Lecture: Some combinatorial aspects of permutation representations

The basic gauge objects of representation theory are the groups $GL(n, k)$, k a field, on the one hand, the symmetric groups S_n on the other, giving rise to *linear representations* respectively *permutation representations*. What is it that makes these groups important representation groups, and do there exist other 'good' representation sequences essentially different from these canonical choices? It is one of the purposes of the theory to be outlined in these lectures to provide a possible answer to these questions in the case of permutation representations. From a technical point of view we are dealing with an enumerative theory yielding both precise and asymptotic results on certain generalized Frobenius numbers. These results are of interest in their own right, but also lead to a number of important applications in other parts of group theory. In order to gain some feeling for the above questions as well as for the type of enumerative formulae to be encountered in this context, it will be helpful to first turn to permutation representations.

For a group Γ denote by $s_n(\Gamma)$ the number of subgroups of index n in Γ. If Γ is finitely generated or of finite subgroup rank, then $s_n(\Gamma)$ is finite for all $n \geq 1$. There is a (more or less) well-known connection between the enumeration of Γ–actions on finite sets (i.e. permutation representations of Γ) and the problem of counting finite index subgroups in Γ, manifesting itself in a variety of identities scattered throughout the literature. One of the earliest results in this direction is Marshall Hall's recursion formula[1]

$$s_n(F_r) = n\,(n!)^{r-1} - \sum_{\mu=1}^{n-1} \Big((n-\mu)!\Big)^{r-1} s_\mu(F_r) \tag{1}$$

for the number of index n subgroups in the free group of (finite) rank r. Here, the connection with permutation representations becomes visible if we interpret $(n!)^{r-1}$ and $((n-\mu)!)^{r-1}$ as values of the function $|\mathrm{Hom}(F_r, S_m)|/(m!)$. Formula (1) was generalized by I.M.S. Dey to free products; cf. [11, Theorem 6.10]. Denote by $\iota_m(H)$ the number of solutions of the equation $x^m = 1$ in a finite group H; i.e., $\iota_m(H) = |\mathrm{Hom}(C_m, H)|$, where C_m is the cyclic group of order m. Chowla, Herstein, and Scott [10] obtain the exponential generating function of the sequence $\{\iota_m(S_n)\}_{n=0}^\infty$ as

$$\sum_{n=0}^\infty \iota_m(S_n)\, z^n/n! = \exp\left(\sum_{d|m} z^d/d\right). \tag{2}$$

Here, the subgroup numbers of C_m appear as silent factors 1 in the sum comprising the exponent. This is apparent from the more general relation

$$\sum_{n=0}^\infty |\mathrm{Hom}(G, S_n)|\, z^n/n! = \exp\left(\sum_{d|m} s_d(G)\, z^d/d\right), \quad m = |G|, \tag{3}$$

for an arbitrary finite group G. The latter identity, which exhibits the exponential generating function of the sequence $\{|\mathrm{Hom}(G, S_n)|\}_0^\infty$ as a particular type

[1] Cf. [17, Theorem 5.2].

of entire function, was a starting point for the asymptotic enumeration of finite group actions.

Whereas (3) and its generalizations require a more elaborate algebraic proof (to get some idea of the kind of approach working there compare the sketch of proof of Theorem A in the next lecture), identity (2) is easily established by a direct combinatorial argument.

Proof of (2). The number $\iota_m(S_n)$ counts those permutations in S_n whose cycle lengths all divide m. Classify these permutations by the length d (a divisor of m) of the cycle containing the letter 1. Now subdivide the heap of permutations corresponding to the divisor d into subheaps according to the actual d–cycle containing the letter 1. There are

$$\binom{n-1}{d-1}(d-1)! = (n-1)_{d-1}$$

ways of choosing $d-1$ letters out of the set $[n]\backslash\{1\}$ and organizing the resulting d–set into a d–cycle. Thus, the dth heap splits into $(n-1)_{d-1}$ subheaps, each containing $\iota_m(S_{n-d})$ permutations. This yields the equation

$$\sum_{d|m}(n-1)_{d-1}\,\iota_m(S_{n-d}) = \iota_m(S_n), \quad (n \geq 1,\ \iota_m(S_0) = 1).$$

Multiply both sides of this recurrence relation by $z^{n-1}/(n-1)!$, sum over $n \geq 1$, and put $F(z) := \sum_{n=0}^{\infty} \iota_m(S_n) z^n/n!$. Routine manipulations then give

$$F'(z)/F(z) = \sum_{d|m} z^{d-1}$$

with solution

$$F(z) = \exp\left(c + \sum_{d|m} z^d/d\right)$$

for some constant c. Putting $z = 0$ in the latter equation then yields

$$\mathrm{e}^c = F(0) = \iota_m(S_0) = 1,$$

i.e., $c = 0$, whence (2). □

The condition that G should be a finite group can be relaxed considerably: If Γ is a group such that $|\mathrm{Hom}(\Gamma, S_n)| < \infty$ for all $n \geq 0$, then we have the (formal) relation

$$\sum_{n\geq 0} |\mathrm{Hom}(\Gamma, S_n)|\, z^n/n! = \exp\Big(\sum_{n\geq 1} s_n(\Gamma)\, z^n/n\Big). \tag{4}$$

This is a variant of Dey's formula essentially due to Wohlfahrt ; cf. [47]. However, the latter result is not the most general relationship known to hold between these two enumerative aspects of a group. Let Γ be a group, $\Sigma \subseteq \Gamma$ a normal subset of Γ not containing the identity element 1, and let $\Lambda \subseteq \mathbb{N}$ be a set of positive integers. For a set Ω denote by $\mathrm{Hom}_\Sigma^\Lambda(\Gamma, S(\Omega))$ the set of all Γ–actions τ on Ω such that

(i) τ induces a fixed–point–free action of (the elements of) Σ on Ω,

(ii) the lengths of the orbits into which Ω decomposes under τ are contained in the set Λ.

The elements of $\mathrm{Hom}_\Sigma^\Lambda(\Gamma, S(\Omega))$ will be referred to as (Σ,Λ)–*admissible* Γ–actions on Ω. Call a triple (Γ,Σ,Λ) as above *admissible*, if $|\mathrm{Hom}_\Sigma^\Lambda(\Gamma, S_n)| < \infty$ for all $n \geq 0$. If, for instance, Γ is finitely generated or of finite subgroup rank, then the triple (Γ,Σ,Λ) is admissible for each normal subset $\Sigma \subseteq \Gamma - \{1\}$ and every set Λ of positive integers. A subgroup Δ of index n in Γ induces a Γ–action by right multiplication on the n–set $\Delta\backslash\Gamma$ of right cosets, which, after suitable renaming, becomes a Γ–action on $[n]$ with the property that $\mathrm{stab}(1) = \Delta$. Thus, an injective mapping from the set of all index n subgroups of Γ into $\mathrm{Hom}(\Gamma, S_n)$, and if $n = (\Gamma : \Delta) \in \Lambda$ and Δ is such that $\Delta \cap \Sigma = \emptyset$, then the image of Δ under this map will be contained in the subset $\mathrm{Hom}_\Sigma^\Lambda(\Gamma, S_n)$. Hence, admissibility of (Γ,Σ,Λ) implies that the numbers

$$s_\Gamma^\Sigma(n) := \Big|\Big\{\Delta:\ \ \Delta \leq \Gamma,\ (\Gamma:\Delta) = n,\ \Delta\cap\Sigma = \emptyset\Big\}\Big|, \quad n \in \Lambda$$

are finite. For a set $M \subseteq \mathbb{N}_0$ of non–negative integers denote by

$$\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma, S(\Omega))$$

the set of those (Σ, Λ)–admissible Γ–actions on the set Ω whose number of orbits is an element of the set M, and let

$$\mathrm{e}_M(z) := \sum_{n \in M} z^n/n!.$$

Proposition 1. *Let $(\Gamma, \Sigma, \Lambda)$ be an admissible triple, and let $M \subseteq \mathbb{N}_0$ be a set of non–negative integers. Then*

$$\sum_{n \geq 0} |\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma, S_n)|\, z^n/n! = \mathrm{e}_M\bigg(\sum_{n \in \Lambda} s_\Gamma^\Sigma(n)\, z^n/n\bigg). \tag{5}$$

This is [13, Prop. 1]. Or course, putting $\Sigma = \emptyset$, $\Lambda = \mathbb{N}$, and $M = \mathbb{N}_0$, we immediately recover (4). However, introduction of the set Σ allows us to also count special types of subgroups, for instance normal or torsion–free ones, in terms of the corresponding type of group action. As an example, take Γ to be a finitely generated virtually free group, $\Lambda = \mathbb{N}$, $M = \mathbb{N}_0$, and $\Sigma = \mathrm{tor}(\Gamma)\backslash\{1\}$ as the set of non–trivial torsion elements. In this case $s_\Gamma^\Sigma(n)$ is the number of *free* subgroups of index n in Γ, and $|\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma, S_n)|$ counts the *torsion–free* Γ–actions on an n–set, i.e., those Γ–actions on $[n]$ which are free when restricted to finite subgroups.[2] Denoting by m_Γ the least common multiple of the orders of the finite subgroups in Γ

$$|\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma, S_n)| = s_\Gamma^\Sigma(n) = 0, \quad m_\Gamma \nmid n.$$

Letting $a_\Gamma(\lambda) := |\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma, S_{m_\Gamma \lambda})|$ and $b_\Gamma(\lambda) := s_\Gamma^\Sigma(m_\Gamma \lambda)$ we recover from (5) the identity

$$\sum_{\mu=1}^{\lambda} a_\Gamma(\lambda - \mu)\, b_\Gamma(\mu) = m_\Gamma\, \lambda\, a_\Gamma(\lambda), \quad \lambda \geq 1.$$

This relation has been a starting point for a detailed analysis of the growth behaviour and the asymptotics of the function $b_\Gamma(\lambda)$ attached to a finitely generated virtually free group. Finally, here is an application of (5) involving

[2] The fact that torsion–free subgroups of a finitely generated virtually free group are free follows from the structure theorem for these groups due to Serre (in the easier direction) and Karrass/Pietrowski/Solitar; cf. [43, Chap. II, Sect. 2.6, Prop. 11] and [21]. The corresponding result proved in the latter paper relies heavily on the fundamental work [44] of Stallings. See also [12] for a full exposition of the structure theorem, its background, and related material.

non–trivial choices for the sets Λ and M.

How many fixed–point–free $SL(2,\mathbb{Z})$–actions are there on a 10–set having exactly 4 orbits?

Call this number N. In (5) put $\Gamma = SL(2,\mathbb{Z})$, $\Sigma = \emptyset$, $M = \{4\}$, and $\Lambda = \{2,3,4\}$. Then

$$N = \frac{10!}{4!}\left\langle z^{10}, \left(\sum_{n=2}^{4} s_n(\Gamma)\, z^n/n\right)^4\right\rangle. \tag{6}$$

Using the presentation $\Gamma \cong \langle a, b \mid a^4 = b^6 = b^3a^{-2} = 1\rangle$ we find that

$$\begin{aligned} |\mathrm{Hom}(\Gamma, S_1)| &= 1\\ |\mathrm{Hom}(\Gamma, S_2)| &= 2\\ |\mathrm{Hom}(\Gamma, S_3)| &= 12\\ |\mathrm{Hom}(\Gamma, S_4)| &= 96. \end{aligned}$$

Plugging this information into (4) and taking log gives

$$\sum_{n\geq 1} s_n(\Gamma)\, z^n/n = \sum_{\mu\geq 1} (-1)^{\mu-1}\left(z + z^2 + 2z^3 + 4z^4 + \cdots\right)^{\mu}/\mu,$$

from which we read off that $s_2(\Gamma) = 1$, $s_3(\Gamma) = 4$, and $s_4(\Gamma) = 9$. Using these values in (6) gives $N = 573300$.

So far seen a number of counting formulae relating the enumeration of group actions (i.e. ordinary permutation representations) to the computation of subgroup numbers, culminating in a master identity (5) comprising all of today's knowledge concerning this particular problem. We also hinted at the fact that such transformation formulae can be quite useful and have been a starting point for some rather deep investigations concerning, for instance, the asymptotic enumeration of finite group actions or the theory of subgroup growth (we shall return to both these aspects in Lecture V). But learned something more. From a perhaps somewhat philosophical point of view the existence of a formula like (4) means that enumerating permutation representations of a group Γ yields *decodable information* on structural invariants of Γ (in this case subgroup numbers filtered by index). Contrast this property of symmetric groups with the situation for a sequence $\{G_n\}$ of finite groups chosen more or less at random. Generically, the numbers $|\mathrm{Hom}(\Gamma, G_n)|$ will certainly tend to carry some structural information on the group Γ, but in general there will be no way of decoding this information. Indeed, this specific property contributes significantly to the quality of the groups S_n as a representation sequence. In dealing with possible generalizations of permutation representations we will have to start from some class $\mathcal{R}$ of sequences $R_0, R_1, \dots$ of finite groups, which is a fairly natural and technically sufficiently controlled 'neighbourhood' of the sequence $\{S_n\}$, and it is far from clear from the outset what such a class might be. However, our answer to the question posed at the beginning of this lecture (whether there is a 'good' generalization of permutation representations) will also have to depend on the precise meaning attached in this context to the word 'good', i.e., we will have to exhibit a *criterion*, applicable to sequences $\{R_n\} \in \mathcal{R}$, when such a sequence is to be termed a good representation sequence. Building on the above idea we will use the following criterion:

A sequence $\{R_n\} \in \mathcal{R}$ will be termed 'good' if the generating function

$$\sum_{n\geq 0} |\mathrm{Hom}(\Gamma, R_n)|\, z^n/n! \tag{7}$$

can be expressed in terms of the representation sequence $\{R_n\}$ and invariants of Γ for all finitely generated groups Γ.

The question what would be an appropriate and natural choice for the class $\mathcal{R}$ will be taken up in the next lecture.

The Second Lecture: Generalizing permutation representations

The first lecture still leaves us with the task of specifying a class $\mathcal{R}$ of representation sequences $\{R_n\}$, which would form a natural and technically sufficiently controlled environment for pursuing the problem of generalizing permutation representations from the combinatorial point of view outlined at the end of the last lecture; and a priori it is far from clear where to look for an appropriate choice of $\mathcal{R}$. The first hint in this direction (that I am aware of) came in the paper [9] of Chigira. In this paper Chigira studies the equation $x^m = 1$ in finite wreath products of the form $H \wr S_n$ and $H \wr A_n$, and in the Weyl groups W_n of type D_n, obtaining generating functions for the sequences $\{\iota_m(H \wr S_n)\}_{n=0}^{\infty}$, $\{\iota_m(H \wr A_n)\}_{n=0}^{\infty}$, and $\{\iota_m(W_n)\}_{n=0}^{\infty}$. For instance, his result for symmetric wreath products ([9, Theorem 2]) reads

$$\sum_{n=0}^{\infty} \iota_m(H \wr S_n)\, z^n / n! = \exp\left(\sum_{d|m} |H|^{d-1}\, \iota_{m/d}(H)\, z^d / d \right). \tag{8}$$

Chigira's results, limited as they are, nevertheless were the first to point towards the possibility of developing an enumerative theory of wreath product representations generalizing both (5) and Chigira's results in a far reaching and uniform way; a quest which, if successful, at the same time leads to the discovery of a rather natural extension for the concept of permutation representations. It is this theory which we seek to outline in the present lectures. We now proceed to the description of the class $\mathcal{R}$ that we are going to use. Let H be a finite group, $N \trianglelefteq H$ a normal subgroup with H/N abelian, and let $\{\Pi_n\}$ denote the sequence $\{S_n\}$ of symmetric groups or the sequence $\{A_n\}$ of alternating groups. Define

$$(H \wr \Pi_n)_N := \Big\{ (f, \pi) \in H \wr \Pi_n : \ \prod_i f(i) \in N \Big\}, \quad n \geq 0. \tag{9}$$

The process of passing from the full wreath product $H \wr \Pi_n$ to the subgroup $(H \wr \Pi_n)_N$ is referred to as *localisation with respect to* N. If $(H : N) \leq 2$ we call such a localisation *tame*. Our class $\mathcal{R}$ will consist of all sequences $\{R_n\}$ of the form (9). Specific elements of $\mathcal{R}$ are

- symmetric wreath products $H \wr S_n$ ($\Pi_n = S_n$, $N = H$)
- alternating wreath products $H \wr A_n$ ($\Pi_n = A_n$, $N = H$)
- the Weyl groups W_n of type D_n ($\Pi_n = S_n$, $H = C_2$, $N = 1$).

As it turns out, a sequence $\{(H \wr \Pi_n)_N\}$ is a good representation sequence in the sense of our criterion if (and only if) $(H : N) \leq 2$, and our basic counting result, to be explained next, computes the generating function (7) as well as certain refinements of this series whenever $\{R_n\}$ has tame localisation and Γ satisfies some rather mild finiteness assumptions (always met for instance if Γ is finitely generated).

The Main Counting Result

We shall use algebraic multiplication in $S(\Omega)$, i.e., the product $\pi_1 \cdot \pi_2$ of permutations $\pi_1, \pi_2 \in S(\Omega)$ is defined via

$$(\pi_1 \cdot \pi_2)(\omega) := \pi_2(\pi_1(\omega)), \quad \omega \in \Omega.$$

Consequently, group actions on sets will always be right actions, and, for a finite group H and a permutation group $\Pi(\Omega)$ on the finite set Ω, multiplication in the wreath product

$$H \wr \Pi(\Omega) = \Big\{(f, \pi) : \ f : \Omega \to H, \ \pi \in \Pi(\Omega)\Big\}$$

is given by the formulae

$$(f_1, \pi_1) \cdot (f_2, \pi_2) := (f, \pi_1 \cdot \pi_2)$$

$$f(\omega) := f_1(\omega)\, f_2(\pi_1(\omega)), \quad \omega \in \Omega.$$

The canonical projection from $H \wr \Pi(\Omega)$ onto $\Pi(\Omega)$, which picks out the second component, will be denoted by ϵ. Let Γ be a group (finite or infinite), H a finite group, and let $\Sigma \subseteq \Gamma - \{1\}$ be a normal subset of Γ. Moreover, fix a non–empty set $\Lambda \subseteq \mathbb{N}$ of positive integers, and collect all these data into a quadruple $\widehat{Q} = (\Gamma, H, \Sigma, \Lambda)$. Given $\widehat{Q}$ and a finite set Ω we call a homomorphism $\tau : \Gamma \to H \wr S(\Omega)$ (Σ, Λ)*–admissible* if the action $\epsilon\tau$ induced on Ω is (Σ, Λ)–admissible (in the sense explained in Lecture I), and we denote by $\mathrm{Hom}_\Sigma^\Lambda(\Gamma, H \wr S(\Omega))$ the set of all (Σ, Λ)–admissible representations of Γ in $H \wr S(\Omega)$. The quadruple $\widehat{Q}$ itself is termed *admissible* if the set $\mathrm{Hom}_\Sigma^\Lambda(\Gamma, H \wr S_n)$ is finite for every $n \geq 0$. As before, if Γ is finitely generated or of finite subgroup rank, then $\widehat{Q} = (\Gamma, H, \Sigma, \Lambda)$ is admissible for each normal set $\Sigma \subseteq \Gamma - \{1\}$, every finite group H, and every set Λ of positive integers. For a set $M \subseteq \mathbb{N}_0$, an integer $n \geq 0$, and with $\hat{Q}$, $N \trianglelefteq H$, and $\{\Pi_n\}$ as introduced above, we denote by

$$\mathrm{Hom}_{\Sigma}^{\Lambda,M}(\Gamma, (H \wr \Pi_n)_N) \tag{10}$$

the set of those (Σ, Λ)–admissible representations $\tau : \Gamma \to (H \wr \Pi_n)_N$ such that the number of orbits into which $[n]$ decomposes under $\epsilon\tau$ is contained in the set M. If $\widehat{Q}$ is admissible, then the set (10) is finite for each set M of non–negative integers and every $n \geq 0$. Our first main result computes the exponential generating function of the sequence $\{|\mathrm{Hom}_{\Sigma}^{\Lambda,M}(\Gamma, (H \wr \Pi_n)_N)|\}_{n=0}^{\infty}$ whenever the quadruple $\widehat{Q} = (\Gamma, H, \Sigma, \Lambda)$ is admissible, the representation sequence $\{(H \wr \Pi_n)_N\}$ has tame localisation, and Γ satisfies one further very mild finiteness assumption (again implied by finite generation). Before stating this result we take a closer look at its key ingredients.

The series $\Theta_{\Gamma_\Pi}^{\Gamma_N}(z)$. Let $\widehat{Q} = (\Gamma, H, \Sigma, \Lambda)$ be an admissible quadruple, and let $N \trianglelefteq H$ be a normal subgroup with H/N abelian. Given a subgroup Γ' of (finite) index n in Γ, a homomorphism $\chi : \Gamma' \to H$, and a right transversal $\{\gamma_1, \dots, \gamma_n\}$ for Γ' in Γ, define

$$\Gamma_\chi := \Big\{\gamma \in \Gamma : \prod_j \chi(\gamma_j \gamma \overline{\gamma_j \gamma}^{-1}) \in N\Big\},$$

where $\bar{\ } : \Gamma \to \{\gamma_1, \dots, \gamma_n\}$ associates with each element $\gamma \in \Gamma$ the representative $\overline{\gamma}$ of the coset $\Gamma'\gamma$. Consider the map $\psi : \Gamma \to H/N$ sending γ to $\prod_j \chi(\gamma_j \gamma \overline{\gamma_j \gamma}^{-1})N$. Since H/N is abelian, the composition of χ with the canonical projection $H \to H/N$ factors through $\Gamma'/[\Gamma', \Gamma']$ inducing a homomorphism $\chi' : \Gamma'/[\Gamma', \Gamma'] \to H/N$, and $\psi = \chi' \circ V_{\Gamma \to \Gamma'}$, where $V_{\Gamma \to \Gamma'} : \Gamma \to \Gamma'/[\Gamma', \Gamma']$ is the transfer of Γ into Γ'. Since the transfer is a homomorphism and independent of the choice of representatives, the same is true for ψ; consequently, $\Gamma_\chi = \ker(\psi)$ is a normal subgroup of index at most $(H : N)$ in Γ, and is independent of the system of representatives used in its definition. Let $\tau_{\Gamma'} : \Gamma \to S(\Gamma' \backslash \Gamma)$ describe the action of Γ by right multiplication on the set $\Gamma' \backslash \Gamma$ of right cosets of Γ' in Γ, and let $\Pi(\Gamma' \backslash \Gamma)$ be the subgroup of $S(\Gamma' \backslash \Gamma)$ isomorphic to Π_n. Given a positive integer n and two normal subgroups $\Gamma_\Pi, \Gamma_N \trianglelefteq \Gamma$ define

$$s(n, \Gamma_\Pi, \Gamma_N) := \sum_{\substack{(\Gamma:\Gamma')=n \\ \Gamma' \cap \Sigma = \emptyset \\ \tau_{\Gamma'}^{-1}(\Pi(\Gamma' \backslash \Gamma)) = \Gamma_\Pi}} \left|\left\{\chi \in \mathrm{Hom}(\Gamma', H) : \ \Gamma_\chi = \Gamma_N\right\}\right|. \tag{11}$$

As one can show, admissibility of $\widehat{Q}$ implies in particular that the cardinal number (11) is finite for all $n \in \Lambda$ and all normal subgroups $\Gamma_\Pi, \Gamma_N \trianglelefteq \Gamma$. With each pair (Γ_Π, Γ_N) of normal subgroups in Γ we associate a formal power series $\Theta_{\Gamma_\Pi}^{\Gamma_N}(z)$ via

$$\Theta_{\Gamma_\Pi}^{\Gamma_N}(z) := \sum_{n \in \Lambda} |H|^{n-1}\, s(n, \Gamma_\Pi, \Gamma_N)\, z^n/n.$$

Note that if two pairs (Γ_Π, Γ_N) and (Γ'_Π, Γ'_N) of normal subgroups are conjugate under an automorphism of Γ, then $\Theta_{\Gamma_\Pi}^{\Gamma_N}(z) = \Theta_{\Gamma'_\Pi}^{\Gamma'_N}(z)$. The maps $\chi : \Gamma' \to H$ introducted above play a role analogous to that of characters in ordinary representation theory.

The function $\mathbf{\Phi_\Gamma}$. Put $\alpha_\Lambda(\Pi) := \max_{n\in\Lambda}(S_n : \Pi_n)$, and assume that $(H : N) \leq 2$ and that Γ contains only finitely many subgroups of index $\mu_0 := \max(\alpha_\Lambda(\Pi), (H : N))$. Consider the system of subgroup pairs

$$\mathcal{U}_\Gamma := \left\{(\Gamma_\Pi, \Gamma_N) : \ (\Gamma : \Gamma_\Pi) \leq \alpha_\Lambda(\Pi),\ (\Gamma : \Gamma_N) \leq (H : N)\right\},$$

and fix a set $E \subseteq \Gamma$ which generates Γ as a normal subgroup. With each pair $(\Gamma_\Pi, \Gamma_N) \in \mathcal{U}_\Gamma$ we associate a formal variable $z_{(\Gamma_\Pi, \Gamma_N)}$ and a discrete variable $\nu(\Gamma_\Pi, \Gamma_N)$ taking non–negative integral values, and form the power series

$$\Phi_\Gamma\Big(z_{(\Gamma_\Pi,\Gamma_N)};\ (\Gamma_\Pi, \Gamma_N) \in \mathcal{U}_\Gamma\Big) := \sum_\nu \prod_{(\Gamma_\Pi,\Gamma_N)} z_{(\Gamma_\Pi,\Gamma_N)}^{\nu(\Gamma_\Pi,\Gamma_N)}/\nu(\Gamma_\Pi, \Gamma_N)!,$$

where the right–hand sum is extended over those maps $\nu : \mathcal{U}_\Gamma \to \mathbb{N}_0$ satisfying the following $2|E| + 1$ conditions:

$$\begin{cases} \sum\limits_{(\Gamma_\Pi,\Gamma_N)} \nu(\Gamma_\Pi,\Gamma_N) \in M \\ \sum\limits_{e\notin\Gamma_\Pi} \nu(\Gamma_\Pi,\Gamma_N) \equiv 0 \mod \alpha_\Lambda(\Pi), \quad e\in E \\ \sum\limits_{e\notin\Gamma_N} \nu(\Gamma_\Pi,\Gamma_N) \equiv 0 \mod (H:N), \quad e\in E. \end{cases} \tag{12}$$

The function Φ_Γ is called the *exterior function* associated with the data H, N, $\{\Pi_n\}$, Λ, and M. Denote by $\mathcal{J}_\Gamma$ the intersection of all subgroups of index μ_0 in Γ. The quotient $\Gamma/\mathcal{J}_\Gamma$ is an elementary abelian 2–group of rank $\log_2(\sum_{\mu\le\mu_0} s_\mu(\Gamma))$. One can show that the function Φ_Γ does not depend on the choice of the normal generating system E, and that the functions Φ_Γ and $\Phi_{\Gamma/\mathcal{J}_\Gamma}$, formed with respect to the same data $\{\Pi_n\}_0^\infty, H, N, \Lambda$, and M, coincide up to a canonical identification of variables

$$z_{(\Gamma_\Pi,\Gamma_N)} \mapsto z_{(\Gamma_\Pi/\mathcal{J}_\Gamma,\Gamma_N/\mathcal{J}_\Gamma)}, \quad (\Gamma_\Pi,\Gamma_N)\in\mathcal{U}_\Gamma.$$

We shall see later that the exterior function Φ_Γ can be expressed explicitly as an arithmetic mean of truncations of certain exponential functions.

The result. This is the following.

Theorem A ([31, Theorem 1]). *Let $\widehat{Q} = (\Gamma, H, \Sigma, \Lambda)$ be an admissible quadruple, $N \le H$ a subgroup of index $(H:N)\le 2$, $M\subseteq \mathbb{N}_0$ a set of non–negative integers, and let $\{\Pi_n\}$ denote either the sequence $\{S_n\}$ of symmetric groups or the sequence $\{A_n\}$ of alternating groups. Assume that Γ contains only finitely many subgroups of index $\max\big(\alpha_\Lambda(\Pi),(H:N)\big)$. Then*

$$\sum_{n\ge0} |\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma,(H\wr\Pi_n)_N)|\, z^n/n! = \Phi_\Gamma\Big(\Theta_{\Gamma_\Pi}^{\Gamma_N}(z);\ (\Gamma_\Pi,\Gamma_N)\in\mathcal{U}_\Gamma\Big), \tag{13}$$

i.e., the exponential generating function of the sequence $\Big\{|\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma,(H\wr\Pi_n)_N)|\Big\}_0^\infty$ is obtained from the series Φ_Γ by replacing each variable $z_{(\Gamma_\Pi,\Gamma_N)}$ with the corresponding power series $\Theta_{\Gamma_\Pi}^{\Gamma_N}(z)$.

Sketch of the proof. Given a non–empty finite set Ω and two normal subgroups $\Gamma_\Pi,\Gamma_N \trianglelefteq \Gamma$ define $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$ to be the set of all representations $\tau:\Gamma\to H\wr S(\Omega)$ such that

(i) $\epsilon\tau$ is transitive,

(ii) $\epsilon\tau$ is Σ–free (i.e., $\epsilon\tau(\sigma)$ is a fixed–point–free permutation for each $\sigma \in \Sigma$),

(iii) $(\epsilon\tau)^{-1}(\Pi(\Omega)) = \Gamma_\Pi$,

(iv) $\tau^{-1}((H \wr S(\Omega))_N) = \Gamma_N$.

Moreover, given a base point $\omega_0 \in \Omega$, let $U(\Omega, \omega_0)$ denote the subgroup of $H \wr S(\Omega)$ consisting of those elements (f, π) such that $f(\omega_0) = 1$ and $\pi(\omega_0) = \omega_0$. Clearly, $U(\Omega, \omega_0) \cong H \wr S(\Omega - \{\omega_0\})$, and hence

$$|U(\Omega, \omega_0)| = |H|^{|\Omega|-1}\,(|\Omega| - 1)!.$$

The action of $H \wr S(\Omega)$ by conjugation on the set $\mathrm{Hom}(\Gamma, H \wr S(\Omega))$,

$$(\tau \cdot x)(\gamma) := x^{-1}\tau(\gamma)x,$$

for $\tau \in \mathrm{Hom}(\Gamma, H \wr S(\Omega))$, $x \in H \wr S(\Omega)$, and $\gamma \in \Gamma$, restricts to an action of $H \wr S(\Omega)$ (and hence of $U(\Omega, \omega_0)$) on the complex $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$. Furthermore, as a consequence of transitivity, this action of $U(\Omega, \omega_0)$ on $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$ is *free*. Let $\tau : \Gamma \to H \wr S(\Omega)$ be an element of $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$. Then the stabilizer $\Gamma' = \mathrm{stab}_{\epsilon\tau}(\omega_0)$ is a subgroup of index $|\Omega|$ in Γ which avoids Σ, $\Gamma' \cap \Sigma = \emptyset$, and satisfies $\tau_{\Gamma'}^{-1}(\Pi(\Gamma' \backslash \Gamma)) = \Gamma_\Pi$. For $\gamma \in \Gamma$ put $\tau(\gamma) = (f_\gamma, \pi_\gamma)$ and define a map $\chi_\tau : \Gamma' \to H$ via $\chi_\tau(\gamma') := f_{\gamma'}(\omega_0)$. One checks that χ_τ is in fact a homomorphism and that $\chi_{\tau_1} = \chi_{\tau_2}$ if τ_1 and τ_2 are equivalent under the action of $U(\Omega, \omega_0)$. Choose elements $\gamma_\omega \in \Gamma$ such that

$$\epsilon\tau(\gamma_\omega)(\omega_0) = \omega, \quad \omega \in \Omega,$$

and for $\gamma \in \Gamma$ and $\omega \in \Omega$ define $\gamma' \in \Gamma'$ and $\omega' \in \Omega$ by the equation $\gamma_\omega\gamma = \gamma'\gamma_{\omega'}$. Then, for $\gamma \in \Gamma$,

$$\prod_\omega f_\gamma(\omega) \equiv \prod_\omega \chi_\tau(\gamma_\omega\gamma\gamma_{\omega'}^{-1}) \mod N. \tag{14}$$

Combining (14) with the defining property (iv) of $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$, it follows that the homomorphism χ_τ constructed to $\tau \in \mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$ satisfies $\Gamma_{\chi_\tau} = \Gamma_N$. Hence, the assignment $\tau \mapsto \chi_\tau$ induces a map

$$\Psi_{\Gamma_\Pi}^{\Gamma_N}(\Omega,\omega_0) : \frac{\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)}{U(\Omega,\omega_0)} \to \bigcup_{\substack{(\Gamma:\Gamma')=|\Omega| \\ \Gamma'\cap\Sigma=\emptyset \\ \tau_{\Gamma'}^{-1}(\Pi(\Gamma'\backslash\Gamma))=\Gamma_n}} \Big\{\chi \in \mathrm{Hom}(\Gamma', H) :\ \Gamma_\chi = \Gamma_N\Big\}.$$

The most difficult part of the proof (and the part that we are not going to say anything about) is to show that this map $\Psi_{\Gamma_\Pi}^{\Gamma_N}(\Omega,\omega_0)$ is in fact a *bijection*. Assuming this result we roughly proceed as follows. Since $\widehat{Q}$ is admissible, the inclusion

$$\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega) \subseteq \mathrm{Hom}_\Sigma^\Lambda(\Gamma, H \wr S(\Omega)), \quad |\Omega| \in \Lambda$$

shows that $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$ is finite for every set Ω with $|\Omega| \in \Lambda$ and all normal subgroups $\Gamma_\Pi, \Gamma_N \trianglelefteq \Gamma$. Hence, the cardinal numbers $s(n,\Gamma_\Pi,\Gamma_N)$ introduced earlier are finite whenever $n \in \Lambda$, and

$$|\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)| = |H|^{|\Omega|-1}\,(|\Omega|-1)!\, s(|\Omega|,\Gamma_\Pi,\Gamma_N), \quad |\Omega| \in \Lambda. \tag{15}$$

Now think of the set $\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma,(H \wr \Pi_n)_N)$ as being decomposed according to the orbit decomposition associated with its elements τ, and of the maps τ as being decomposed into the disjoint sum of the representations induced by τ on its orbits. Reversing this point of view we construct the elements of $\mathrm{Hom}_\Sigma^{\Lambda,M}(\Gamma,(H \wr \Pi_n)_N)$ by glueing together representations from complexes $\mathcal{RC}_{\Gamma_\Pi}^{\Gamma_N}(\Omega)$ for various sets Ω and normal subgroups $\Gamma_\Pi, \Gamma_N \trianglelefteq \Gamma$. Controlling this process by means of the subgroup pairs (Γ_Π, Γ_N) we can ensure that the resulting representations map Γ into the group $(H \wr \Pi_n)_N$, and the relation (15) is the decisive tool in enumerating the representations constructed in this way.

□

The Third Lecture: Some examples and a formula for the exterior function

In order to familiarize ourselves with different aspects of Theorem A, let us begin by looking at some special cases.

Symmetric wreath products. Putting $\Pi_n = S_n$ and $N = H$ we have $(H \wr \Pi_n)_N = H \wr S_n$, $\alpha_\Lambda(\Pi) = 1$, and $\mathcal{U}_\Gamma = \{(\Gamma, \Gamma)\}$. Dropping the subscript (Γ, Γ), the exterior function Φ_Γ becomes

$$\Phi_\Gamma(z) = \sum_{\nu \in M} z^\nu / \nu! = e_M(z),$$

and Theorem A yields the following.

Corollary. *Let $\widehat{Q} = (\Gamma, H, \Sigma, \Lambda)$ be an admissible quadruple, and let $M \subseteq \mathbb{N}_0$ be a set of non-negative integers. Then*

$$\sum_{n \geq 0} |\mathrm{Hom}_\Sigma^{\Lambda, M}(\Gamma, H \wr S_n)|\, z^n / n! = e_M\biggl(\sum_{n \in \Lambda} |H|^{n-1}\, s_{\Gamma,\Sigma}^H(n)\, z^n / n \biggr), \tag{16}$$

where $s_{\Gamma,\Sigma}^H(n) := \sum_{\substack{(\Gamma:\Gamma')=n \\ \Gamma' \cap \Sigma = \emptyset}} |\mathrm{Hom}(\Gamma', H)|.$

Letting $H = 1$ in (16) we recover Proposition 1, the main counting result for permutation representations, together with all its applications. If, on the other hand, we let $\Gamma = G$ and H be arbitrary finite groups, $|G| = m$, and put $\Sigma = \emptyset$, $\Lambda = \mathbb{N}$, and $M = \mathbb{N}_0$, then we find that

$$\sum_{n=0}^{\infty} |\mathrm{Hom}(G, H \wr S_n)|\, z^n / n! = \exp\biggl(\sum_{d \mid m} |H|^{d-1}\, s_G^H(d)\, z^d / d \biggr), \tag{17}$$

where $s_G^H(d) := s_{G,\emptyset}^H(d) = \sum_{(G:U)=d} |\mathrm{Hom}(U, H)|$. This is a generalization of formula (3) to symmetric wreath products. For $G = C_m$ a cyclic group of order m, formula (17) specializes to Chigira's result (8) mentioned at the beginning of Lecture II. For the dihedral group

$$D = D_\ell = \langle w, \sigma \mid w^\ell = \sigma^2 = 1,\ \sigma w \sigma = w^{-1} \rangle$$

of order $m = 2\ell$ the picture is slightly more involved. Let d be a divisor of m. If $d \mid \ell$ then D contains d dihedral subgroups of order m/d, namely the groups

$$U_i = \langle w^d, w^i \sigma \rangle, \quad 0 \leq i < d.$$

Also, if d is even, D has one cyclic subgroup of index d, namely $U = \langle w^{d/2} \rangle$. Hence,

$$s_D^H(d) = \begin{cases} d\,|\mathrm{Hom}(D_{\ell/d}, H)|; & d \equiv 1\ (2) \\ \iota_{m/d}(H); & d \equiv 0\ (2), d \not| \, l \\ \iota_{m/d}(H) + d\,|\mathrm{Hom}(D_{\ell/d}, H)|; & d \equiv 0\ (2), d \mid l, \end{cases}$$

and, by (17)

$$\sum_{n=0}^{\infty} |\mathrm{Hom}(D_\ell, H \wr S_n)|\, z^n/n! = \exp\left(\frac{1}{|H|} \sum_{d|\ell} |\mathrm{Hom}(D_{\ell/d}, H)|\,(|H|z)^d + \frac{1}{2|H|} \sum_{d|\ell} \iota_{\ell/d}(H)\,(|H|z)^{2d}/d \right). \quad (18)$$

Alternating wreath products. In Theorem A put $\Pi_n = A_n$, $N = H$, $\Sigma = \emptyset$, $\Lambda = \mathbb{N}$, and $M = \mathbb{N}_0$. Then $(H \wr \Pi_n)_N = H \wr A_n$, and the set $\mathcal{U}_\Gamma$ can be identified with the system of all subgroups of index at most 2 in Γ. Let $\Gamma = G = \langle \zeta \rangle$ be a cyclic group of order m with m even. Then there are two subgroups of index at most 2 in G, $G_1 = G$ and $G_2 = \langle \zeta^2 \rangle$, and we denote by z_1, ν_1 respectively z_2, ν_2 their associated variables. Put $E = \{\zeta\}$. Our exterior function Φ_G takes the form

$$\Phi_G(z_1, z_2) = \sum_{\substack{\nu_1, \nu_2 \geq 0 \\ \nu_2 \equiv 0(2)}} \frac{z_1^{\nu_1} z_2^{\nu_2}}{\nu_1! \nu_2!} = \exp(z_1) \cosh(z_2) = \frac{1}{2} \left\{ \mathrm{e}^{z_1 + z_2} + \mathrm{e}^{z_1 - z_2} \right\}.$$

For $d \mid m$ consider the subgroup $U = \langle \zeta^d \rangle$ of index d in G. The generator ζ acts on the coset space $U \backslash G$ as the d-cycle $\tau_U(\zeta) = (U \cdot 1, U \cdot \zeta, \ldots, U \cdot \zeta^{d-1})$. Consequently, we have $\tau_U(G) \subseteq A(U \backslash G)$ if and only if d is odd. From this we see that

$$s(d, G_1, G) = \begin{cases} \iota_{m/d}(H), & \text{d odd} \\ 0, & \text{d even} \end{cases}$$

and

$$s(d, G_2, G) = \begin{cases} \iota_{m/d}(H), & \text{d even} \\ 0, & \text{d odd.} \end{cases}$$

It follows that

$$\begin{aligned} \Theta_1(z) &:= \Theta_{G_1}^G(z) = \sum_{\substack{d|m \\ d\equiv 1(2)}} |H|^{d-1}\,\iota_{m/d}(H)\,z^d/d, \\ \Theta_2(z) &:= \Theta_{G_2}^G(z) = \sum_{\substack{d|m \\ d\equiv 0(2)}} |H|^{d-1}\,\iota_{m/d}(H)\,z^d/d, \end{aligned}$$

and, by Theorem A

$$\sum_{n=0}^{\infty} \iota_m(H \wr A_n)\,z^n/n! = \frac{1}{2}\left\{\exp\left(\sum_{d|m} |H|^{d-1}\,\iota_{m/d}(H)\,z^d/d\right)\right. \\ \left. + \exp\left(\sum_{d|m} (-|H|)^{d-1}\,\iota_{m/d}(H)\,z^d/d\right)\right\}. \quad (19)$$

For odd m this equation coincides with (8). Thus, we have obtained [9, Theorem 4]. The special case of (19) where $H = 1$ and $m = 2$ is already found in [25, Sect. 5]. As another example let us consider the Klein 4–group $G = C_2^2 = \langle \zeta, \eta \rangle$. Here, the exterior function Φ_G occurring in the enumeration of alternating representations will depend on four variables z_0, z_ζ, z_η, $z_{\zeta\eta}$, corresponding to the four subgroups $G_0 = G$, $G_\zeta = \langle \zeta \rangle$, $G_\eta = \langle \eta \rangle$, and $G_{\zeta\eta} = \langle \zeta\eta \rangle$. Note that G_ζ, G_η, and $G_{\zeta\eta}$ are equivalent under $\mathrm{Aut}(G)$. Let $E = \{\zeta, \eta\}$. We have

$$\Phi_G(z_0, z_\zeta, z_\eta, z_{\zeta\eta}) = \sum_{\substack{\nu_0, \nu_\zeta, \nu_\eta, \nu_{\zeta\eta} \geq 0 \\ \nu_\zeta + \nu_{\zeta\eta} \equiv 0(2) \\ \nu_\eta + \nu_{\zeta\eta} \equiv 0(2)}} \frac{z_0^{\nu_0} z_\zeta^{\nu_\zeta} z_\eta^{\nu_\eta} z_{\zeta\eta}^{\nu_{\zeta\eta}}}{\nu_0!\,\nu_\zeta!\,\nu_\eta!\,\nu_{\zeta\eta}!} =$$

$$\exp(z_0)\Big[\cosh(z_\zeta)\cosh(z_\eta)\cosh(z_{\zeta\eta}) + \sinh(z_\zeta)\sinh(z_\eta)\sinh(z_{\zeta\eta})\Big] =$$

$$\frac{1}{4}\left\{e^{z_0 + z_\zeta + z_\eta + z_{\zeta\eta}} + e^{z_0 + z_\zeta - z_\eta - z_{\zeta\eta}} + e^{z_0 - z_\zeta + z_\eta - z_{\zeta\eta}} + e^{z_0 - z_\zeta - z_\eta + z_{\zeta\eta}}\right\}.$$

Something interesting happens in the last step: by expanding the hyperbolic functions in terms of exponential functions we obtain 16 terms, 8 of which cancel, with the remaining ones occurring in pairs. We will come back to the latter phenomenon and the problem of explicitly computing the exterior function Φ_Γ in general at the end of this lecture. It remains to compute the interior functions $\Theta_0(z)$, $\Theta_\zeta(z)$, $\Theta_\eta(z)$, and $\Theta_{\zeta\eta}(z)$ corresponding to the variables z_0, z_ζ, z_η, $z_{\zeta\eta}$ respectively. We have

$$s(d, G_0, G) = \begin{cases} |\mathrm{Hom}(C_2^2, H)|, & \mathrm{d} = 1 \\ 0, & \mathrm{d} = 2 \\ 1, & \mathrm{d} = 4 \end{cases}$$

and

$$s(d, G_\zeta, G) = \begin{cases} \iota_2(H), & \mathrm{d} = 2 \\ 0, & \text{otherwise.} \end{cases}$$

This gives

$$\begin{aligned} \Theta_0(z) &= |\mathrm{Hom}(C_2^2, H)|\, z + \frac{|H|^3}{4} z^4, \\ \Theta_\zeta(z) &= \Theta_\eta(z) = \Theta_{\zeta\eta}(z) = \frac{|H|\, \iota_2(H)}{2} z^2, \end{aligned}$$

and hence, by Theorem A

$$\sum_{n=0}^{\infty} |\mathrm{Hom}(C_2^2, H \wr A_n)|\, z^n/n! = \frac{1}{4} \left(\sum_{n=0}^{\infty} |\mathrm{Hom}(C_2^2, H \wr S_n)|\, z^n/n! \right) \times \left\{ 1 + 3\exp(-2\,|H|\,\iota_2(H)\, z^2) \right\},$$

where

$$\sum_{n=0}^{\infty} |\mathrm{Hom}(C_2^2, H \wr S_n)| z^n/n! = \exp\left(|\mathrm{Hom}(C_2^2, H)| z + \frac{3\,|H| \iota_2(H)}{2} z^2 + \frac{|H|^3}{4} z^4 \right);$$

cf. formula (18).

The Weyl groups of type D_n. If we put $\Pi_n = S_n$, $H = C_2$, and $N = 1$, then $(H \wr \Pi_n)_N = W_n$ is the Weyl group of the (crystallographic) root system of type D_n. Consider again the cyclic group $\Gamma = G = \langle \zeta \rangle$ of order m with m even, and let $\Sigma = \emptyset$, $\Lambda = \mathbb{N}$, and $M = \mathbb{N}_0$. Keeping the previous notation, the set $\mathcal{U}_\Gamma$ can again be identified with the set $\{G_1, G_2\}$, and, as before

$$\Phi_G(z_1, z_2) = \frac{1}{2}\left\{e^{z_1+z_2} + e^{z_1-z_2}\right\}.$$

For $d \mid m$ consider the subgroup $U = \langle \zeta^d \rangle$ of index d in G and a character $\chi : U \to C_2$. If m/d is odd then $\chi \equiv 1$, and $G_\chi = G_1$. If, on the other hand, m/d is even, then there are two characters $\chi : U \to C_2$: the trivial character $\chi_0 \equiv 1$ with $G_{\chi_0} = G_1$, and a non-trivial character χ_1. In the latter case

$$\prod_{j=1}^{d} \chi_1(\zeta^j \overline{\zeta^j}^{-1}) = \chi_1(\zeta^d) \neq 1,$$

i.e., $\zeta \notin G_{\chi_1}$, and hence $G_{\chi_1} = G_2$. We conclude that

$$s(d, G, G_1) = 1 \quad (d \mid m) \quad \text{and} \quad s(d, G, G_2) = \begin{cases} 1, & \text{m/d even} \\ 0, & \text{m/d odd.} \end{cases}$$

It follows that

$$\Theta_1(z) = \sum_{d \mid m} 2^{d-1} z^d/d \quad \text{and} \quad \Theta_2(z) = \sum_{\substack{d \mid m \\ m/d \equiv 0(2)}} 2^{d-1} z^d/d,$$

and hence

$$\sum_{n=0}^{\infty} \iota_m(W_n) z^n/n! = \frac{1}{2} \exp\left(\sum_{\substack{d \mid m \\ m/d \equiv 1(2)}} \frac{2^{d-1}}{d} z^d \right) \left\{ 1 + \exp\left(\sum_{\substack{d \mid m \\ m/d \equiv 0(2)}} \frac{2^d}{d} z^d \right) \right\}.$$

Again, this formula also holds for odd m in virtue of (8), and we have found [9, Theorem 5]. The corresponding result for the Klein 4–group is that

$$\sum_{n=0}^{\infty} |\mathrm{Hom}(C_2^2, W_n)| \, z^n/n! = \frac{1}{4} \exp\left(4z + 6z^2 + 2z^4\right)\left\{1 + 3\,e^{-4z}\right\}.$$

Calculation of Φ_Γ. A decisive step for the further development of our theory is the explicit computation of the exterior function Φ_Γ. As remarked in the previous lecture, Φ_Γ does not depend on the (normal) generating system of Γ used in its definition, and its calculation may be performed in the finite group $\Gamma/\mathcal{J}_\Gamma$, where $\mathcal{J}_\Gamma$ denotes the intersection of all subgroups of index $\mu_0 = \max(\alpha_\Lambda(\Pi), (H:N))$ in Γ. Put

$$\mathcal{U}_\Gamma^+ := \Big\{\Gamma' :\ \Gamma' \leq \Gamma,\ (\Gamma:\Gamma') \leq \mu_0\Big\},$$

and let $\pi : \Gamma \to \Gamma/\mathcal{J}_\Gamma$ be the canonical projection. The quotient $V = \Gamma/\mathcal{J}_\Gamma$ is an elementary abelian 2–group of rank $r = \log_2\left(\sum_{\mu\leq\mu_0} s_\mu(\Gamma)\right)$, which we view as a vector space over the field $k = GF(2)$ with two elements. Let E be the standard basis of V, and let $\langle\cdot,\cdot\rangle$ be the usual inner product on V with respect to E, i.e., $\langle u, v\rangle = \sum u_i v_i$. We define a map $\hat{}: V \to \mathcal{U}_\Gamma^+$ via $\hat{v} := \pi^{-1}(v^\perp)$. Its inverse is the map $^- : \mathcal{U}_\Gamma^+ \to V$ given by $\overline{\Gamma} = \mathsf{o}$ and $\overline{\Gamma'} = v$ with $v \neq \mathsf{o}$ and $\langle v, x\rangle = 0$ for all $x \in \pi(\Gamma')$ if $(\Gamma:\Gamma') = 2$. Under this bijection the set $\mathcal{U}_\Gamma$ is identified with the subspace

$$\mathcal{U}_V = V_{\alpha_\Lambda(\Pi)} \oplus V_{(H:N)}$$

of dimension $R = r\Big(\log_2 \alpha_\Lambda(\Pi) + \log_2(H:N)\Big)$ in $V \oplus V$, where $V_1 := \{\mathsf{o}\}$ and $V_2 := V$. The standard basis of $\mathcal{U}_V$ is $\mathcal{E} = \mathcal{U}_V \cap ((E \times V_1) \cup (V_1 \times E))$. The inner product on V induces the inner product

$$\langle (u,v),(x,y)\rangle = \langle u,x\rangle + \langle v,y\rangle$$

on $V \oplus V$, and, hence, on $\mathcal{U}_V$. Denote by $\Phi_V = \Phi_V\Big(z_{(u,v)};\ (u,v) \in \mathcal{U}_V\Big)$ the power series obtained from Φ_Γ by replacing each variable $z_{(\Gamma_\Pi,\Gamma_N)}$ and $\nu(\Gamma_\Pi,\Gamma_N)$ with the corresponding variable $z_{(u,v)}$ respectively $\nu(u,v)$, where $\hat{u} = \Gamma_\Pi$ and $\hat{v} = \Gamma_N$. Moreover, for a set $M \subseteq \mathbb{N}_0$ of non–negative integers and a (formal) power series $f(z_1,\ldots,z_s) = \sum_{\nu_1,\ldots,\nu_s\geq 0} a_{\nu_1,\ldots,\nu_s} z_1^{\nu_1}\ldots z_s^{\nu_s}$, denote by $[f(z_1,\ldots,z_s)]_M$ the truncation

$$\Big[f(z_1,\ldots,z_s)\Big]_M = \sum_{\substack{\nu_1,\ldots,\nu_s\geq 0\\ \nu_1+\cdots+\nu_s\in M}} a_{\nu_1,\ldots,\nu_s}\, z_1^{\nu_1}\ldots z_s^{\nu_s}$$

of f with respect to M. The following result provides an explicit formula for

Φ_V, and hence also for the function Φ_Γ.

Theorem B ([34, Theorem 3.1]). *We have*

$$\Phi_V = \frac{1}{|\mathcal{U}_V|}\sum_{(u,v)\in\mathcal{U}_V}\left[\exp\left(\sum_{\langle(x,y),(u,v)\rangle=0} z_{(x,y)} - \sum_{\langle(x,y),(u,v)\rangle=1} z_{(x,y)}\right)\right]_M.$$

Sketch of the proof. Up to truncation with respect to M,

$$\Phi_V = \sum_\nu \prod_{(u,v)\in\mathcal{U}_V} z_{(u,v)}^{\nu(u,v)}\big/\nu(u,v)!,$$

where the right–hand sum is extended over the maps $\nu : \mathcal{U}_V \to \mathbb{N}_0$ such that

$$\sum_{\langle(x,y),(u,v)\rangle=1} \nu(x,y) \equiv 0 \quad (2), \quad (u,v)\in\mathcal{E}. \tag{20}$$

For a map $\nu \in k^{\mathcal{U}_V}$ let

$$S = S(\nu) := \Big\{(u,v)\in\mathcal{U}_V : \nu(u,v) = 1\Big\}.$$

Viewing (20) as a system of equations over k, a map $\nu : \mathcal{U}_V \to k$ is a solution of (20) if and only if

$$\sum_{(u,v)\in S}(u,v) = (o,o).$$

Hence, introducing the set

$$\mathcal{S}_0 := \left\{S\subseteq\mathcal{U}_V : \sum_{(u,v)\in S}(u,v) = (o,o),\ (o,o)\notin S\right\},$$

and blowing up the solutions of (20) over k to maps $\nu : \mathcal{U}_V \to \mathbb{N}_0$ we obtain the following description of the function Φ_V:

$$\Phi_V = \mathrm{e}^{z_{(o,o)}}\sum_{S\in\mathcal{S}_0}\prod_{(u,v)\in S}\sinh(z_{(u,v)})\prod_{(u,v)\in\mathcal{U}_V^\sharp\setminus S}\cosh(z_{(u,v)}), \tag{21}$$

where $\mathcal{U}_V^\sharp := \mathcal{U}_V - \{(o,o)\}$. Expanding the hyperbolic functions in terms of exponential functions, (21) can be rewritten as

$$\Phi_V = \mathrm{e}^{z_{(o,o)}}\sum_{\varepsilon\in\{\pm1\}^{\mathcal{U}_V^\sharp}} C_\varepsilon \exp\left(\sum_{(u,v)\in\mathcal{U}_V^\sharp}\varepsilon(u,v)z_{(u,v)}\right) \tag{22}$$

with certain coefficients $C_\varepsilon \in \mathbb{Z}\left[\frac{1}{2^{2^R-1}}\right]$. For a sign function $\varepsilon : \mathcal{U}_V^\sharp \to \{\pm 1\}$ define

$$\begin{aligned} E_+(\varepsilon) &:= \left\{ S \in \mathcal{S}_0 : \; |\{(u,v) \in S : \varepsilon(u,v) = -1\}| \equiv 0 \mod 2 \right\} \\ E_-(\varepsilon) &:= \mathcal{S}_0 - E_+(\varepsilon). \end{aligned}$$

Then

$$\begin{aligned} C_\varepsilon &= 2^{-|\mathcal{U}_V^\sharp|} \sum_{S \in \mathcal{S}_0} (-1)^{|\{(u,v)\in S :\, \varepsilon(u,v)=-1\}|} \\ &= 2^{-(2^R-1)} \Big(|E_+(\varepsilon)| - |E_-(\varepsilon)| \Big). \end{aligned} \tag{23}$$

Next, one shows that (i) if $E_-(\varepsilon) \neq \emptyset$ then $C_\varepsilon = 0$ (by setting up a bijection between $E_+(\varepsilon)$ and $E_-(\varepsilon)$ in this case), and (ii) $|\mathcal{S}_0| = 2^{2^R - R - 1}$. Combining (22) and (23) with (i) and (ii) we find that

$$\Phi_V = 2^{-R}\, \mathrm{e}^{z_{(o,o)}} \sum_{\substack{\varepsilon \in \{\pm 1\}^{\mathcal{U}_V^\sharp} \\ E_+(\varepsilon) = \mathcal{S}_0}} \exp\Bigg(\sum_{(u,v) \in \mathcal{U}_V^\sharp} \varepsilon(u,v)\, z_{(u,v)} \Bigg).$$

The proof of Theorem B is then completed by showing that the sign functions $\varepsilon : \mathcal{U}_V^\sharp \to \{\pm 1\}$ satisfying $E_+(\varepsilon) = \mathcal{S}_0$ are precisely those obtained from some subspace $H \leq \mathcal{U}_V$ of codimension ≤ 1 by putting

$$\varepsilon_H(u,v) = \begin{cases} +1, & (u,v) \in H - \{(o,o)\} \\ -1, & (u,v) \in \mathcal{U}_V - H. \end{cases}$$

Indeed, let H be a hyperplane in $\mathcal{U}_V$, and let S be a subset of $\mathcal{U}_V^\sharp$. Then we have

$$\sum_{(u,v) \in S \cap (\mathcal{U}_V - H)} (u,v) \in H \quad \text{if and only if} \quad |S \cap (\mathcal{U}_V - H)| \equiv 0 \bmod 2,$$

and hence

$$\sum_{(u,v) \in S} (u,v) \in H \quad \text{if and only if} \quad |\{(u,v) \in S : \; \varepsilon_H(u,v) = -1\}| \equiv 0 \bmod 2;$$

in particular, ε_H satisfies $E_+(\varepsilon_H) = \mathcal{S}_0$. The converse statement, to the effect that a non–trivial sign function ε satisfying $E_+(\varepsilon) = \mathcal{S}_0$ must come (in the sense defined above) from some hyperplane of $\mathcal{U}_V$, is less obvious. □

The Fourth Lecture: Explicit formulae for abelian groups and computations in Quillen complexes

Combining Theorems A and B with results from the theory of Hall polynomials, it is possible to derive explicit formulae for the generating functions $\sum_{n\geq 0} |\mathrm{Hom}(G, R_n)| z^n/n!$, where G is a finite abelian group and the representation sequence $\{R_n\}$ is any of $\{H \wr S_n\}$ or $\{H \wr A_n\}$ with a fixed finite group H, or $\{W_n\}$. This is a much more formidable task than, say, the derivation of Chigira's corresponding results on finite cyclic groups (cf. Lecture III), and serves well to illustrate some of the power of Theorems A and B. Unfortunately, it is also a lengthy and rather technical subject matter, and time does not permit us to enter into much detail here. Instead, what I have chosen to talk about in the present lecture is a fascinating link between such formulae and the topology of certain Quillen complexes. Specifically, we will see how explicit identities for elementary abelian groups may be used to produce an efficient and extremely fast algorithm for computing the Euler characteristic of Quillen complexes associated with members of one of the representation sequences mentioned above. The identities our algorithm is based upon are as follows. First,

$$\begin{aligned}\sum_{n=0}^{\infty} |\mathrm{Hom}(C_p^r, H \wr S_n)| z^n/n! &= \\ &= \exp\left(\frac{1}{|H|}\sum_{\rho=0}^{r} p^{-\rho}\binom{r}{\rho}_p |\mathrm{Hom}(C_p^{r-\rho}, H)|(|H|z)^{p^\rho}\right).\end{aligned} \tag{24}$$

Here p is a prime, r a non–negative integer, H a finite group, and the p–binomial coefficient $\binom{r}{\rho}_p$ is, by definition, the number of ρ–dimensional subspaces in an r–dimensional vector space over $GF(p)$. It is well known that

$$\binom{r}{\rho}_p = \prod_{j=0}^{\rho-1} \frac{p^{r-j}-1}{p^{\rho-j}-1}.$$

Second, we have

$$\sum_{n=0}^{\infty}|\mathrm{Hom}(C_2^r, H\wr A_n)|z^n/n! = 2^{-r}\left(\sum_{n=0}^{\infty}\frac{|\mathrm{Hom}(C_2^r, H\wr S_n)|}{n!}z^n\right)$$
$$\times\left\{1+(2^r-1)\exp\left(-\frac{2^{r-1}}{|H|}|\mathrm{Hom}(C_2^{r-1}, H)|(|H|z)^2\right)\right\}, \tag{25}$$

and finally

$$\sum_{n=0}^{\infty}|\mathrm{Hom}(C_2^r, W_n)|z^n/n! =$$
$$= 2^{-r}\left(\sum_{n=0}^{\infty}\frac{|\mathrm{Hom}(C_2^r, C_2\wr S_n)|}{n!}z^n\right)\left\{1+(2^r-1)\mathrm{e}^{-2^r z}\right\}. \tag{26}$$

Of course, for p odd

$$|\mathrm{Hom}(C_p^r, H\wr A_n)| = |\mathrm{Hom}(C_p^r, H\wr S_n)|, \quad n\geq 0$$

and

$$|\mathrm{Hom}(C_p^r, W_n)| = |\mathrm{Hom}(C_p^r, C_2\wr S_n)|, \quad n\geq 0.$$

We begin by recalling some definitions and outlining the basic strategy underlying our approach.

The basic strategy. Let P be a finite partially ordered set, and let $\mathfrak{A}(P)$ be its associated (real) incidence algebra, i.e., the set of all functions $f: P\times P\to\mathbb{R}$ such that $f(x,y)=0$ if $x\not\leq y$, with pointwise addition and scalar multiplication, and multiplication $*$ defined by

$$(f*g)(x,y) = \sum_{x\leq z\leq y} f(x,z)\,g(z,y). \tag{27}$$

$\mathfrak{A}(P)$ is an associative $\mathbb{R}$–algebra with (two–sided) identity δ given by

$$\delta(x,y) = \begin{cases} 1, & x=y\\ 0, & x\neq y.\end{cases}$$

It is easy to see from the definition (27) that an element $f\in\mathfrak{A}(P)$ has a left (right, two–sided) inverse if and only if $f(x,x)\neq 0$ for all $x\in P$. The Möbius function μ_P is defined as the inverse of the zeta function ζ_P of P, the latter being given by

$$\zeta_P(x,y) = \begin{cases} 1, & x \le y \\ 0, & \text{otherwise.} \end{cases}$$

The order complex $\Delta(P)$ of P is, by definition, the abstract simplicial complex whose k–dimensional simplices are the chains $x_0 < \ldots < x_k$ from P. The reduced Euler characteristic $\tilde{\chi}(\Delta(P))$ of $\Delta(P)$ is defined as $\tilde{\chi}(\Delta(P)) = \sum_i (-1)^i f_i$, where f_i denotes the number of i–dimensional simplices of $\Delta(P)$. Since $\Delta(P)$ contains precisely one simplex of dimension -1 (the empty chain), $\tilde{\chi}(\Delta(P))$ is related to the ordinary Euler characteristic $\chi(\Delta(P))$ by $\tilde{\chi}(\Delta(P)) = \chi(\Delta(P)) - 1$. For a finite group G and a prime p define $\mathcal{S}_p(G)$ to be the poset of all non–trivial p–subgroups of G, ordered by inclusion. Similarly, define $\mathcal{A}_p(G)$ as the subposet of $\mathcal{S}_p(G)$ whose elements are the non–trivial p–tori of G, i.e., the non–trivial elementary abelian p–subgroups of G. The complexes $\Delta(\mathcal{S}_p(G))$ and $\Delta(\mathcal{A}_p(G))$ appeared first in the work of Brown (see [6] and [7]) on Euler characteristics and cohomology of discrete groups, and their homotopy properties were studied in some detail by Quillen around 1976; cf. [40]. Quillen showed, among other things, that geometric realizations of these two complexes are homotopy equivalent, and that they are contractible if G has a normal p–subgroup. Moreover, he conjectured that the converse of the last result holds. One of his main results ([40, Theorem 12.1]) implies the truth of this conjecture in the case that G is soluble. In general, Quillen's conjecture is still open, although significant progress has been made using the classification of finite simple groups (see [3]). Here, we focus on the computation of the (reduced) Euler characteristic of these complexes for certain families of groups G.

By a result of P. Hall (see [18, (2.21)] or [41, Prop. 3.6]) the reduced Euler characteristic of $\Delta(P)$ and the Möbius function on P are related by

$$\tilde{\chi}(\Delta(P)) = \mu_{\hat{P}}(\hat{0}, \hat{1}),$$

where $\hat{P}$ is the poset obtained by adding a minimum element $\hat{0}$ and a maximum element $\hat{1}$ to P. By the definition of the Möbius function,

$$\tilde{\chi}(\Delta(P)) = - \sum_{x \in P \cup \{\hat{0}\}} \mu_{\hat{P}}(\hat{0}, x).$$

In particular, if $P = \mathcal{A}_p(G)$, we can think of $\hat{0}$ as the trivial subgroup $1 \leq G$. Then, if $T \leq G$ is a p–torus of rank r, we have (see [18, (2.7)] or [41, Ex. 5.2])

$$\mu_{\widehat{\mathcal{A}_p(G)}}(1, T) = \mu_{\mathcal{L}(T)}(1, T) = (-1)^r \, p^{\binom{r}{2}},$$

where $\mathcal{L}(T)$ denotes the lattice of all subgroups of T. Hence, the problem of determining $\tilde{\chi}(\Delta(\mathcal{A}_p(G)))$ is reduced to the problem of enumerating the p–tori in G by rank. For an arbitrary group G this is difficult. However, if we know $|\mathrm{Hom}(C_p^r, G)|$ for each positive integer r, then we can use Möbius inversion on the lattice of subgroups of C_p^r to determine the number $|\mathrm{Inj}(C_p^r, G)|$ of embeddings of C_p^r in G. The number of p–tori in G of rank r is then obtained by dividing $|\mathrm{Inj}(C_p^r, G)|$ by the order of $\mathrm{Aut}(C_p^r) = \mathrm{GL}(r, p)$. The inversion process just described together with certain analytic considerations explained below produces an expression for $\tilde{\chi}(\Delta(\mathcal{A}_p(G)))$ as an infinite series (formula (32)), but we can use this series representation together with a result of K. Brown to produce a finite algorithm which finds the desired Euler characteristic. Of course, the efficiency of this algorithm depends on being able to quickly compute the values $|\mathrm{Hom}(C_p^r, G)|$. If G is a member of one of the representation sequences $\{H \wr S_n\}$ or $\{H \wr A_n\}$ with some finite group H whose associated function $|\mathrm{Hom}(C_p^r, H)|$ is known, or if G is one of the Weyl groups W_n, formulae (24) – (26) provide exactly this information.

The algorithm (outline). We shall need three series–product identities discovered by Euler in his investigations relating to partitions.[3] The first of these identities is

$$1 + \sum_{n=1}^{\infty} p(n) \, q^n = \prod_{n=1}^{\infty} (1 - q^n)^{-1}, \quad |q| < 1, \tag{28}$$

[3] Cf. [14, Chap. 16].

which exhibits the generating function $P(q) = 1 + \sum_{n=1}^{\infty} p(n)\, q^n$ for $p(n)$, the number of unrestricted partitions of n, as an infinite product. The other two are

$$1 + \sum_{n=1}^{\infty} \frac{t^n}{(1-q)(1-q^2)\cdots(1-q^n)} = \prod_{n=0}^{\infty} (1 - t\, q^n)^{-1}, \tag{29}$$

and

$$1 + \sum_{n=1}^{\infty} \frac{t^n\, q^{\binom{n}{2}}}{(1-q)(1-q^2)\cdots(1-q^n)} = \prod_{n=0}^{\infty} (1 + t\, q^n), \tag{30}$$

where in both cases we have absolute convergence for $|t| < 1$ and $|q| < 1$. Formulae (29) and (30) can be given interpretations in terms of partitions with restriction as to the number of their parts; see [1, Chap. 2, Ex. 17]. Both are special cases of the q–binomial theorem; cf. for instance [15, Sect. 1.3] or [2, Sect. 10.2]. Now define two functions $F(z)$ and $G(z)$ by

$$F(z) := 1 + \sum_{n=1}^{\infty} \frac{z^{\binom{n}{2}}}{(z-1)(z^2-1)\cdots(z^n-1)}$$

respectively

$$G(z) := 1 + \sum_{n=1}^{\infty} \frac{1}{(1-z)(1-z^2)\cdots(1-z^n)}.$$

Setting $t = q = 1/z$ in (29) gives

$$F(z) = \prod_{n=1}^{\infty} (1 - (1/z)^n)^{-1},$$

which, when combined with (28), shows that $F(z)$ is absolutely convergent for $|z| \notin (0,1]$, and that for $|z| > 1$ we have $F(z) = P(1/z)$. If, on the other hand, we put $t = -q$ and $q = 1/z$ in (30), then we find that $G(z)$ is absolutely convergent for $|z| > 1$, and that

$$G(z) = \prod_{n=1}^{\infty} (1 - (1/z)^n), \quad |z| > 1.$$

Combining the latter equation with (28) and the fact that $F(z) = P(1/z)$ finally shows that

$$F(z)\, G(z) = 1, \quad |z| > 1.$$

These are the facts concerning the functions $F(z)$ and $G(z)$ we are going to use.

By establishing the estimate

$$\frac{|\mathrm{Hom}(C_p^{k+1}, G)| / \prod_{j=1}^{k+1}(p^j-1)}{|\mathrm{Hom}(C_p^k, G)| / \prod_{j=1}^{k}(p^j-1)} \leq \frac{1}{p^{k-r_p(G)+1}-1}, \quad k \geq r_p(G) \tag{31}$$

one shows that the series

$$\sum_{k=0}^{\infty} (-1)^k \frac{|\mathrm{Hom}(C_p^k, G)|}{\prod_{j=1}^{k}(p^j-1)}$$

is absolutely convergent for every finite group G and each prime p. Here, $r_p(G)$ denotes the p–rank of G, i.e., the maximum over the ranks of the p–tori in G. Next we claim the following.

Proposition 2 ([35]). *For every prime p and each finite group G we have*

$$-\tilde{\chi}(\Delta(\mathcal{A}_p(G))) = P(1/p) \sum_{k=0}^{\infty} (-1)^k \frac{|\mathrm{Hom}(C_p^k, G)|}{\prod_{j=1}^{k}(p^j-1)}. \tag{32}$$

Proof. By the previous observations, the right–hand side of (32) is (absolutely) convergent, and we have

$$\begin{aligned} P(1/p) \sum_{k=0}^{\infty}(-1)^k \frac{|\mathrm{Hom}(C_p^k, G)|}{\prod_{j=1}^{k}(p^j-1)} &= \sum_{s=0}^{\infty} \frac{p^{\binom{s}{2}}}{\prod_{j=1}^{s}(p^j-1)} \sum_{k=0}^{\infty}(-1)^k \frac{|\mathrm{Hom}(C_p^k, G)|}{\prod_{j=1}^{k}(p^j-1)} \\ &= \sum_{k=0}^{\infty}(-1)^k \frac{|\mathrm{Hom}(C_p^k, G)|}{\prod_{j=1}^{k}(p^j-1)} \sum_{r\geq k} \frac{p^{\binom{r-k}{2}}}{\prod_{j=1}^{r-k}(p^j-1)} \\ &= \sum_{r=0}^{\infty} \sum_{k=0}^{r} (-1)^k \frac{|\mathrm{Hom}(C_p^k, G)| p^{\binom{r-k}{2}}}{\prod_{j=1}^{k}(p^j-1) \prod_{j=1}^{r-k}(p^j-1)}. \end{aligned}$$

For $r \geq 0$, let $T(p, r, G)$ denote the number of p–tori in G which have rank r. We have

$$-\tilde{\chi}(\Delta(\mathcal{A}_p(G))) = \sum_{r\geq 0} (-1)^r \, p^{\binom{r}{2}} \, T(p, r, G),$$

and

$$T(p, r, G) = \frac{|\mathrm{Inj}(C_p^r, G)|}{|GL(r, p)|} = \frac{|\mathrm{Inj}(C_p^r, G)|}{p^{\binom{r}{2}} \prod_{j=1}^{r}(p^j-1)}.$$

Let $V \cong C_p^r$. Then

$$|\mathrm{Hom}(V, G)| = \sum_{W \leq V} |\mathrm{Inj}(V/W, G)| = \sum_{W \leq V} |\mathrm{Inj}(W, G)|,$$

the last equality following from duality in the lattice of subspaces of V. By Möbius inversion, we find that

$$|\mathrm{Inj}(V,G)| = \sum_{W\le V} \mu(W,V)\,|\mathrm{Hom}(W,G)| = \sum_{k=0}^{r} (-1)^{r-k}\, p^{\binom{r-k}{2}} \binom{r}{k}_p |\mathrm{Hom}(C_p^k,G)|,$$

whence (32). □

Equation (32) is an interesting representation of $\tilde{\chi}(\Delta(\mathcal{A}_p(G)))$ as an (absolutely convergent) infinite series, but, as it stands, it is of course not sufficient to produce a finite algorithm. However, by truncating the series on the right–hand side of (32), estimating the remainder by means of (31), and applying a result of Brown [6] to the effect that $\tilde{\chi}(\Delta(\mathcal{A}_p(G))) \in p\mathbb{Z}$, we obtain the following.

Theorem C ([35]). *Let G be a finite group, and let p be a prime. Define*

$$\kappa(p,G) := \min\left\{k \ge r_p(G) : \frac{|\mathrm{Hom}(C_p^k,G)|}{\prod_{j=1}^{k}(p^j-1)} < \frac{p}{2P(1/p)}\right\}.$$

Then

$$-\tilde{\chi}(\Delta(\mathcal{A}_p(G))) = \left[P(1/p) \sum_{k=0}^{\kappa(p,G)-1} (-1)^k \frac{|\mathrm{Hom}(C_p^k,G)|}{\prod_{j=1}^{k}(p^j-1)}\right]_p, \tag{33}$$

where for $x \in \mathbb{R}\backslash\frac{p}{2}\mathbb{Z}$, $[x]_p$ denotes the integer multiple of p which is closest to x.

Theorem C, when combined with formulae (24) – (26) provides a finite and fast algorithm for computing the Euler characteristic of the Quillen complex $\Delta(\mathcal{A}_p(G))$ when G is part of one of the representation sequences mentioned earlier, after the following two details are handled:

(i) Formula (33) involves $P(1/p)$, so we must be able to efficiently compute this value for each given prime p. However, evaluating the function $G(z)$ at $z=p$ gives an alternating series rapidly converging to $1/P(1/p)$.

(ii) In order to determine $\kappa(p,G)$ one must know $r_p(G)$. The following lemma gives $r_p(G)$ in terms of $r_p(H)$ when G is one of the groups $H\wr S_n$ or $H\wr A_n$ with some finite group H, and also gives $r_p(W_n)$. The results below are probably well known, but I have been unable to find an explicit reference other than [35].

Lemma 3 ([35]). *Let $n \in \mathbb{N}$, and let p be a prime. Then*

(a) $r_p(S_n) = \lfloor n/p \rfloor$.

(b) $r_p(A_n) = \begin{cases} r_p(S_n) - 1, & p = 2 \text{ and } n \equiv 2, 3\,(4) \\ r_p(S_n), & \text{otherwise.} \end{cases}$

(c) *Let H be any finite group, and let Π_n be one of A_n or S_n. Then*

$$r_p(H \wr \Pi_n) = \begin{cases} r_p(\Pi_n), & r_p(H) = 0 \\ r_p(H)n, & r_p(H) > 0. \end{cases}$$

(d) $r_p(W_n) = \begin{cases} r_p(S_n), & p > 2 \\ n, & p = 2 \text{ and } n \equiv 0\,(2) \\ n - 1, & p = 2 \text{ and } n \equiv 1\,(2). \end{cases}$

The Fifth Lecture: Asymptotics of $|\mathrm{Hom}(G, H \wr S_n)|$ and subgroup growth

Having dealt with the exact enumeration of generalized permutation representations it appears natural to ask about the asymptotic behaviour of arithmetic functions of the form $|\mathrm{Hom}(\Gamma, R_n)|$, where $\{R_n\}$ is a representation sequence of the type considered in Theorem A. Here, we will focus on the special case where $\Gamma = G$ is a finite group and $R_n = H \wr S_n$ for some finite group H, which has a distinct complex analytic flavour. This case in particular incorporates the problem of asymptotically enumerating finite group actions, which has received considerable attention since the early 1950's, and was finally settled by myself in 1995.[4] Another interesting feature of this special case is its connection with the theory of subgroup growth: sufficiently precise estimates for the function $|\mathrm{Hom}(G, H \wr S_n)|$ with arbitrary G and H can be translated into asymptotic

[4]See [46] or [30, Sect. 1] for some remarks concerning the history of that problem.

information on the function $s_\Gamma^H(n) = \sum_{(\Gamma:\Gamma')=n} |\mathrm{Hom}(\Gamma', H)|$ for a large class of virtually free groups Γ. We will illustrate this important aspect by deriving an asymptotic formula for the function $s_\Gamma^H(n)$ in the case when Γ is a free product of the form

$$\Gamma = G_1 * \cdots * G_s * F_r \tag{34}$$

with $r, s \geq 0$ and non–trivial finite groups G_σ.

The function $|\mathrm{Hom}(G, H \wr S_n)|$. In view of formula (17) the problem of obtaining asymptotic estimates for the arithmetic function in question is a special case of the following.

($\mathcal{P}$) *Given a real polynomial $P(z)$, derive asymptotic information on the Laurent coefficients α_n of the entire function* $\exp(P(z)) = \sum_0^\infty \alpha_n z^n$, *which is explicit in $P(z)$ and n.*

Problem ($\mathcal{P}$) was studied already around 1920 by Pólya [39] in connection with his investigation concerning the zeros of the derivatives of certain analytic functions. His result is however not sufficiently explicit for our purposes. Also, Pólya's method does not give complete asymptotic expansions, but only partial information on the first term. In the case $P(z) = z$, a solution of ($\mathcal{P}$) is, of course, given by Stirling's formula

$$n! \sim (2\pi)^{1/2}\, n^{n+1/2}\, \mathrm{e}^{-n} \quad (n \to \infty), \tag{35}$$

or, on a higher level of precision, by the expansion

$$n! \approx (2\pi)^{1/2}\, n^{n+1/2}\, \mathrm{e}^{-n} \left\{1 + \sum_{\nu=1}^{\infty} \mathfrak{c}_\nu\, \mathfrak{n}^{-\nu}\right\} \quad (\mathfrak{n} \to \infty) \tag{36}$$

of factorials derived from Stirling's asymptotic expansion of $\log \Gamma(z)$. As is well known, the coefficients $\mathfrak{c}_\nu$ in (36) can be expressed in terms of Bernoulli numbers via the (formal) identity

$$\exp\left(\sum_{k=1}^{\infty} \frac{B_{2k}}{2k(2k-1)}\, z^{-(2k-1)}\right) = 1 + \sum_{\nu=1}^{\infty} \mathfrak{c}_\nu\, z^{-\nu}. \tag{37}$$

In dealing with the function $|\mathrm{Hom}(G, H \wr S_n)|$ the crux is to obtain results for $(\mathcal{P})$ analogous to (35) or (36) for a sufficiently large class of polynomials including in particular all polynomials

$$P_G^H(z) = \sum_{d|m} \frac{|H|^{d-1} s_G^H(d)}{d}\, z^d, \quad m = |G|$$

associated with a pair (G, H) of finite groups, while maintaining this high level of explicitness in $P(z)$ and n. Indeed, interpreted in this rather strict sense, $(\mathcal{P})$ is not a well–posed problem, since the class of functions $\left\{e^{P(z)} : P(z) \in \mathbb{R}[z]\right\}$ turns out to be too large to allow for a uniform asymptotic behaviour of the coefficients α_n. Hence, we have to investigate problem $(\mathcal{P})$ under certain technical restrictions on the polynomial $P(z)$, which on the one hand should be flexible enough to accommodate a sufficiently large class of polynomials, while on the other hand being stringent enough to enforce uniform asymptotic behaviour of the α_n. Let $P(z) = \sum_{\mu=1}^{m} c_\mu z^\mu$ with $c_m \neq 0$. Two important such conditions in our context are Hayman's condition

(H) $\qquad \alpha_n > 0$ for sufficiently large n

and the gap condition

(G) $\qquad c_\mu = 0$ for $m/2 < \mu < m$.

Condition (H) can be rephrased in terms of $P(z)$ as follows: $P(z)$ meets condition (H) if and only if (i) $\gcd(\mathrm{supp}(P)) = 1$, and (ii) $c_{\max(supp(P)\cap(\mathbb{Z}-d\mathbb{Z}))} > 0$ for every integer $d > 1$. Here $\mathrm{supp}(P) := \{\mu \in \mathbb{N} : c_\mu \neq 0\}$ is the support of $P(z)$. The gap condition (G) has turned out to be the most efficient way of exploiting the fact that the polynomials $P_G^H(z)$ have the property that

$$\mathrm{supp}(P_G^H) \subseteq \left\{d : d \mid \deg(P_G^H(z))\right\}.$$

Indeed, it is this condition which allows us to obtain completely explicit estimates for polynomials of arbitrary degree. The following result, which provides a generalization of Stirling's formula (35), conveys some of the flavour of my investigations concerning problem $(\mathcal{P})$.

Theorem D ([30, Theorem 1]). *Suppose that the polynomial* $P(z)$ *meets conditions* (G) *and* (H). *Then the coefficients* α_n *of the entire function* $\exp(P(z))$ *satisfy the asymptotic formula*

$$\alpha_n \sim \frac{K}{\sqrt{2\pi n}}\, n_0^{-n/m}\, \exp\left(P(n_0^{1/m})\right) \quad (n \to \infty), \tag{38}$$

where $n_0 := n/(mc_m)$ and

$$K = K(P) := \begin{cases} m^{-1/2}, & m \text{ odd} \\ m^{-1/2} \exp\left(-\frac{c_{m/2}^2}{8c_m}\right), & m \text{ even.} \end{cases}$$

Sketch of the proof. Our starting point in proving Theorem D is the asymptotic formula

$$\alpha_n \sim \frac{\exp\left(P(r_n)\right)}{r_n^n \sqrt{2\pi m n}} \quad (n \to \infty), \tag{39}$$

in terms of the positive real root r_n (for sufficiently large n) of the equation $rP'(r) = n$, which follows from Hayman's work [20]. In order to turn (39) into an explicit asymptotic formula we have to approximate r_n by a function ρ_n (which is explicit in n and $P(z)$) with sufficient precision to allow r_n^n and $\exp(P(r_n))$ to be estimated asymptotically also, i.e., $r_n^n \sim \rho_n^n$ and $\exp(P(r_n)) \sim \exp(P(\rho_n))$. For this we will need r_n with an (absolute) error of order $o(n^{-1+1/m})$. Let

$$\Phi(z) := \left(\sum_{\mu=1}^{m} \mu\, c_\mu\, z^{m-\mu}\right)^{1/m} \underset{z\neq 0}{=} \left(z^{m-1}\, P'(1/z)\right)^{1/m}.$$

Applying Lagrange inversion to the equation $w\,\Phi(z) = z$ and substituting $w = n^{-1/m}$ and $z = r^{-1}$, we find that

$$\frac{1}{r_n} \approx \beta_1\, n^{-1/m} \left\{1 + \sum_{\nu=1}^{\infty} \beta_1^{-1} \frac{\beta_{\nu+1}}{\nu+1}\, n^{-\nu/m}\right\} \quad (n \to \infty), \tag{40}$$

where

$$\beta_\nu = \left\langle z^{\nu-1},\, (\Phi(z))^\nu \right\rangle, \quad \nu \geq 1, \tag{41}$$

i.e., β_ν is the coefficient of $z^{\nu-1}$ in the expansion of $(\Phi(z))^\nu$ around the origin. Define a function ρ_n by

$$\rho_n := \beta_1^{-1} n^{1/m} \left\{ 1 + \sum_{\nu=1}^{m} \beta_1^{-1} \frac{\beta_{\nu+1}}{\nu+1} n^{-\nu/m} \right\}^{-1}.$$

Clearly, ρ_n is well–defined for sufficiently large n, and, by (40), $r_n = \rho_n + O(n^{-1})$, hence

$$\alpha_n \sim \frac{\exp(P(\rho_n))}{\rho_n^n \sqrt{2\pi m n}} \quad (n \to \infty). \tag{42}$$

Note that so far we have only used assumption (H) (to ensure (39)). Expanding $(\Phi(z))^\nu = (m\,c_m)^{\nu/m} (1 + \sum_{\mu=1}^{m-1} \frac{\mu c_\mu}{m c_m} z^{m-\mu})^{\nu/m}$ we infer from (41) plus the gap condition (G) that (i) $\beta_1 = (m\,c_m)^{1/m}$, (ii) $\beta_\nu = 0$ for $1 < \nu < m/2+1$, and (iii) that

$$\beta_{m/2+1} = \frac{m+2}{4}\, c_{m/2}\, (m\,c_m)^{-\frac{m-2}{2m}}, \quad 2 \mid m. \tag{43}$$

Abbreviating the sum $\sum_{m/2 \le \nu \le m} \beta_1^{-1} \frac{\beta_{\nu+1}}{\nu+1} n^{-\nu/m}$ as Σ, and using the fact that Σ is of order $O(n^{-\lceil m/2 \rceil/m})$, we find that as $n \to \infty$

$$\rho_n^{-n} = n_0^{-n/m} (1+\Sigma)^n = n_0^{-n/m} \exp\Big(n\Sigma - \sigma^2/2 + o(1)\Big),$$

i.e.,

$$\rho_n^{-n} \sim n_0^{-n/m} \exp\Big(n\Sigma - \sigma^2/2\Big) \quad (n \to \infty), \tag{44}$$

where

$$\sigma := \begin{cases} \frac{2}{m+1}\, \beta_1^{-1}\, \beta_{m/2+1}, & m \text{ even} \\ 0, & m \text{ odd.} \end{cases}$$

In order to rewrite $\exp(P(\rho_n))$ we have to deal with the terms $\exp(\rho_n^\mu)$ for $1 \le \mu \le m/2$ and $\mu = m$. First, it is immediate from the definition of ρ_n that

$$\exp(\rho_n^\mu) \sim \exp(n_0^{\mu/m}), \quad 1 \le \mu \le \left\lfloor \frac{m-1}{2} \right\rfloor. \tag{45}$$

So, it remains to deal with the case $\mu = m$ for m odd and the cases $\mu = m/2, m$ for even m. For m even and $\mu = m$, the most complex subcase, we find that as $n \to \infty$

$$\rho_n^m = n_0 (1+\Sigma)^{-m} = n_0 - c_m^{-1}\, n\,\Sigma + \frac{m+1}{2\,c_m} \sigma^2 + o(1),$$

and hence

$$\exp(\rho_n^m) \sim \exp\left(n_0 - c_m^{-1}\, n\, \Sigma + \frac{m+1}{2\, c_m}\, \sigma^2\right) \quad (n \to \infty,\ 2 \mid m). \tag{46}$$

In a similar way we find that

$$\exp(\rho_n^{m/2}) \sim \exp\left(n_0^{1/2} - \frac{m}{2\sqrt{m\, c_m}}\, \sigma\right) \quad (n \to \infty,\ 2 \mid m) \tag{47}$$

and

$$\exp(\rho_n^m) \sim \exp\left(n_0 - c_m^{-1}\, n\, \Sigma\right) \quad (n \to \infty,\ 2 \not\mid m). \tag{48}$$

Taking into account formulae (42), (43), (44), (45), (46), (47), and (48) we obtain (38). □

Applying Theorem D and Stirling's formula to the identity (17) gives

$$|\mathrm{Hom}(G, H \wr S_n)| \sim$$
$$K_G^H\, (|H|\, n)^{(1-1/m)n} \exp\left(-\frac{m-1}{m}\, n + \frac{1}{|H|} \sum_{\substack{d \mid m \\ d < m}} \frac{s_G^H(d)}{d}\, (|H|\, n)^{d/m} \right), \tag{49}$$

where $m = |G|$ and

$$K_G^H = \begin{cases} m^{-1/2}, & m \text{ odd} \\ m^{-1/2} \exp\left(- \frac{(s_G(m/2)\iota_2(H))^2}{2m|H|} \right), & m \text{ even.} \end{cases}$$

A noteworthy consequence of (49) is that for finite groups G_1 and G_2,

$$|\mathrm{Hom}(G_1, S_n)| \sim |\mathrm{Hom}(G_2, S_n)| \;\Rightarrow\; |\mathrm{Hom}(G_1, S_n)| = |\mathrm{Hom}(G_2, S_n)|,\ n \geq 0.$$

This phenomenon is referred to as 'asymptotic stability' of finite groups. Under more stringent conditions on the polynomial $P(z)$ (still met by the polynomials $P_G^H(z)$), the asymptotic formula (38) can in fact be extended to a full asymptotic expansion of α_n; cf. [30, Theorem 2]. The latter result should be viewed as an analogue of Stirling's expansion (36) and the identity (37) for polynomials of higher degree. Its proof, which is based on the work of Harris and Schoenfeld [19], is several orders of magnitude harder than that of Theorem D, and the result itself is too technical to be stated here. However, as a consequence of these developments, a complete asymptotic expansion of the function $|\mathrm{Hom}(G, H \wr S_n)|$ is obtained for arbitrary G and H of the form right–hand side of (49) times a Poincaré series in $(|H|n)^{-1/m}$, with coefficients given explicitly in terms of m, $|H|$, and the $s_G^H(d)$; cf. [31, Theorem 4].

Subgroup growth of free products. Let Γ be a free product of the form (34), $m_\sigma := |G_\sigma|$ for $1 \leq \mu \leq s$, H a finite group, and put $h_\Gamma^H(n) := |\mathrm{Hom}(\Gamma, H \wr S_n)|/(n!)$. Then, by (49) and Stirling's formula,

$$h_\Gamma^H(n) \sim L_\Gamma^H \, |H|^{n-1} \, n^{-1} \, \Phi_\Gamma^H(n) \quad (n \to \infty), \tag{50}$$

where

$$L_\Gamma^H := (2\pi)^{\frac{r-1}{2}} \, (m_1 \ldots m_s)^{-1/2} \, |H| \exp\Bigg(- \frac{\big(\iota_2(H)\big)^2}{|H|} \sum_{\substack{\sigma \\ 2|m_\sigma}} \frac{\big(s_{G_\sigma}(m_\sigma/2)\big)^2}{2m_\sigma} \Bigg) \tag{51}$$

and

$$\Phi_\Gamma^H(n) := \big(|H|n\big)^{-\chi(\Gamma)n} \exp\Bigg(\chi(\Gamma)\, n \, + \frac{1}{|H|} \sum_{\sigma=1}^{s} \sum_{\substack{d_\sigma | m_\sigma \\ d_\sigma < m_\sigma}} \frac{s_{G_\sigma}^H(d_\sigma)}{d_\sigma} \big(|H|n\big)^{d_\sigma/m_\sigma} + \frac{r+1}{2} \log n\Bigg). \tag{52}$$

Note that, by results of Kurosh and Baer/Levi, the numbers r,s, and the groups G_σ (up to order and isomorphism) are isomorphism invariants of Γ (cf. for example [22, §35]). If Γ is as in (34), then its Euler characteristic (in the sense of Wall) is given by[5]

$$\chi(\Gamma) = \sum_{\sigma=1}^{s} \frac{1}{m_\sigma} - r - s + 1.$$

Putting $\Sigma = \emptyset$, $\Lambda = \mathbb{N}$, and $M = \mathbb{N}_0$ in formula (16) we find that the functions $h_\Gamma^H(n)$ and $\tilde{s}_\Gamma^H(n) := |H|^{n-1} s_\Gamma^H(n)$ are related by the transformation formula

$$n \, h_\Gamma^H(n) = \sum_{k=1}^{n} \tilde{s}_\Gamma^H(k) \, h_\Gamma^H(n-k), \quad n \geq 1. \tag{53}$$

[5] Cf. [8, Chap. IX, Prop. 7.3] or [42, Prop. 14].

Hall's formula (1) for free groups is a special case of this. In order to discuss the asymptotic behaviour of the function $s_\Gamma^H(n)$ we adopt, for a moment, the following more formal point of view. Consider two sequences $1 = h_0, h_1, h_2, \ldots$ and $s_1, s_2, s_3, \ldots$ of real numbers satisfying a relation

$$\sum_{k=1}^{n} s_k\, h_{n-k} = c\, n\, h_n, \quad n \geq 1 \tag{54}$$

with some constant $c > 0$. We require that $s_n \geq 0$ and $h_n > 0$ for $n \geq 1$. Define the *triangle* $\Delta = (H_k^n)_{0 \leq k \leq n}$ *associated with the transformation* (54) by

$$H_k^n := \frac{h_n}{h_k\, h_{n-k}}, \quad 0 \leq k \leq n,$$

and for each fixed integer $K \geq 1$ put

$$A_n^{(K)} := \sum_{k=K}^{n-K} (H_k^n)^{-1}.$$

For the application we have in mind both sequences $\{h_n\}$ and $\{s_n\}$ grow super-exponentially fast. This means that generating functions associated with these sequences are purely formal, which would seem to suggest that nothing can be accomplished here by analytic means. However, a general philosophy – well known for instance in probability theory – states that if the growth of the sequences involved is *much faster* than the growth of the transformation between them (which in our case is exponential), then asymptotic information can be *transferred* from one sequence to the other. The simplest result in this direction is the following observation of Wright, which allows us to derive an asymptotic formula for the sequence s_n once we are given an asymptotic formula for h_n.

Lemma 1 ([48, Theorem 3]). *If in the context of* (54) *we have* $A_n^{(1)} \to 0$ *as* $n \to \infty$, *then* $s_n \sim c\, n\, h_n$.

Furthermore, combining the estimate (50) with methods from Real Analysis, one can show the following.

Lemma 2 ([32]). *Suppose that* $\chi(\Gamma) < 0$, *let* H *be a finite group, and let* $K \geq 1$

be a fixed natural number. Then as $n \to \infty$

$$\sum_{k=K}^{n-K} \frac{h_\Gamma^H(k)\, h_\Gamma^H(n-k)}{h_\Gamma^H(n)} = O(n^{K\,\chi(\Gamma)}). \tag{55}$$

Formulae (50) and (53) in conjunction with Lemmas 1 and 2 now yield the following.

Theorem E ([32]). *Let* Γ *be a free product of the form* (34) *with* $\chi(\Gamma) < 0$, *and let* H *be a finite group. Then we have*

$$s_\Gamma^H(n) \sim L_\Gamma^H\, \Phi_\Gamma^H(n) \quad (n \to \infty), \tag{56}$$

where L_Γ^H *and* $\Phi_\Gamma^H(n)$ *are given by* (51) *respectively* (52).

This is a generalization of [29, formula (30)]. As an example, consider the modular group $\Gamma = PSL(2,\mathbb{Z})$. Here $r = 0$, $s = 2$, $m_1 = 2$, $m_2 = 3$, and $\chi(\Gamma) = -1/6$, and Theorem E gives

$$s_{PSL(2,\mathbb{Z})}^H(n) \sim \frac{|H| \exp\Big(-\frac{(\iota_2(H))^2}{4|H|}\Big)}{2\sqrt{3}\pi} \Big(|H|n\Big)^{n/6} \exp\Big(-\frac{n}{6} + \Big(\frac{n}{|H|}\Big)^{1/2} + \Big(\frac{n}{|H|^2}\Big)^{1/3} + \frac{1}{2}\log n\Big). \tag{57}$$

There exists a more elaborate asymptotic method for divergent power series due to E. M. Wright [49] and – in greater generality – to E. A. Bender [5], which involves the sums $A_n^{(K)}$ for all $K \geq 1$, and allows us, in the context of (54), to derive a full asymptotic expansion for the function s_n from a known expansion of the sequence h_n. This method, when combined with a full asymptotic expansion of the function $h_\Gamma^H(n)$, yields a complete expansion for $s_\Gamma^H(n)$ of the form $L_\Gamma^H\, \Phi_\Gamma^H(n)$ times a Poincaré series in $(|H|n)^{-1/m_\Gamma}$, whose coefficients are given explicitly in terms of Γ and H. The latter result in turn is a decisive tool in attacking a long standing problem going back to Klein and Poincaré concerning the asymptotic distribution of the isomorphism types of subgroups in the modular group and other free products. Consider again the (inhomogeneous) modular group $\Gamma = \mathrm{PSL}(2,\mathbb{Z}) \cong C_2 * C_3$. By Kurosh's subgroup theorem, any subgroup $\Gamma' \leq \Gamma$ is of the form

$$\Gamma' \cong \underbrace{C_2 * \ldots * C_2}_{\lambda} * \underbrace{C_3 * \ldots * C_3}_{\mu} * F_\nu$$

with non–negative integers λ, μ, and ν. Hence, the isomorphism type of a subgroup $\Gamma' \leq \Gamma$ is conveniently described by means of the triple $t(\Gamma') = (\lambda, \mu, \nu) \in \mathbb{N}_0^3$. Moreover, if Γ' has finite index in Γ, then an Euler characteristic calculation shows that $t(\Gamma')$ and $(\Gamma : \Gamma')$ are connected via the relation

$$3\,\lambda \,+\, 4\,\mu \,+\, 6\,(\nu - 1) = (\Gamma : \Gamma').$$

The problem to construct, classify, and enumerate finite index subgroups in the modular group with given restrictions on the isomorphism type goes back to Klein and Poincaré, and has received a large amount of attention since the 1880's, both as an intrinsic problem for the modular group, and in connection with the construction of modular forms; cf. for example [4], [16], [23], [24], [36], [37], [38], [45], and the literature cited therein. Despite these enormous efforts, not too much appears to be known concerning the asymptotic behaviour of the arithmetic functions associated with these counting problems. Denote by $a_\Gamma(\lambda, \mu, \nu)$ the number of finite index subgroups $\Gamma' \leq \Gamma$ such that $t(\Gamma') = (\lambda, \mu, \nu)$, let $t_i = (\lambda_i, \mu_i, \nu_i) \in \mathbb{N}_0^3$ be a sequence of isomorphism types such that $n_i := 3\lambda_i + 4\mu_i + 6(\nu_i - 1) \to \infty$ as $i \to \infty$, and consider the function $a_\Gamma(t_i)$. Then the Klein–Poincaré problem asks: what can we say about the sequence $\{a_\Gamma(t_i)\}_1^\infty$, in particular what is its growth behaviour and asymptotics? If $t_i = (0, 0, \nu_i)$ with $\nu_i \geq 2$ and $\nu_i \to \infty$ as $i \to \infty$, then the general results obtained in [26], [27], and [28] concerning torsion–free subgroups of finite index in finitely generated virtually free groups apply; for example we find from [27, Theorem 5] that

$$a_\Gamma(t_i) \sim \frac{3}{\pi}\, 6^{\nu_i - 1}\, (\nu_i \,-\, 1)! \quad (i \to \infty).$$

Consider the equation

$$s_\Gamma^H(n) = \sum_{\substack{\lambda,\mu,\nu \geq 0\\ 3\lambda+4\mu+6(\nu-1)=n}} \Big(\iota_2(H)\Big)^\lambda \Big(\iota_3(H)\Big)^\mu |H|^\nu\, a_\Gamma(\lambda, \mu, \nu) \tag{58}$$

with Γ and n fixed, and varying H. Then the set of triples (λ, μ, ν) (and thus also the values of the function a_Γ) involved in the right–hand sum will remain the same, while the coefficient $(\iota_2(H))^\lambda(\iota_3(H))^\mu|H|^\nu$ varies with H, as does the left–hand side $s_\Gamma^H(n)$. Hence, by varying H we are able to produce sufficiently many independent equations of the form (58) to solve for the a_Γ's in terms of the functions $s_\Gamma^H(n)$. This in turn allows us to bring the asymptotic formula (56) given in Theorem E respectively its refinement [32, Theorem 1] to bear on the above problem, which, in conjunction with techniques for the approximation of sums, leads to asymptotic estimates for the function $a_\Gamma(t_i)$ for a large class of sequences $\{t_i\}$ of isomorphism types. Moreover, this strategy is, of course, not confined to the modular group, but can be used to systematically investigate the corresponding more general problem for free products of the form (34) and some of their lifts; cf. [32] and [33].

References

[1] Andrews, G., *The theory of partitions*, Cambridge University Press, 1998.

[2] Andrews, G., Askey, R.; Roy, R., *Special functions*, Encyclopedia of Mathematics and its Applications Vol. 71, Cambridge University Press, 1999.

[3] Aschbacher, M.; Smith, S., *On Quillen's conjecture for the p–groups complex*, Ann. of Math. 137 (1993), 473 – 529.

[4] Atkin, A. O. L.; Swinnerton–Dyer, H. P. F., *Modular forms on non–congruence subgroups*, Amer. Math. Soc. Symposium on Combinatorics, Los Angeles, 1971.

[5] Bender, E. A., *An asymptotic expansion for the coefficients of some formal power series*, J. London Math. Soc. 9 (1975), 451–458.

[6] Brown, K., *Euler characteristics of groups: The p–fractional part*, Invent. Math. 29 (1975), 1 – 5.

[7] Brown, K., *High–dimensional cohomology of discrete groups*, Proc. Nat. Acad. Sci. USA 73 (1976), 1795 – 1797.

[8] Brown, K., *Cohomology of groups*, Springer, New York, 1982.

[9] Chigira, N., *The solutions of* $x^d = 1$ *in finite groups*, J. Algebra 180 (1996), 653 – 661.

[10] Chowla, S.; Herstein, I. N.; Scott, W. R., *The solutions of* $x^d = 1$ *in symmetric groups*, Norske Vid. Selsk. 25 (1952), 29 – 31.

[11] Dey, I., *Schreier systems in free products*, Proc. Glasgow Math. Soc. 7 (1965), 61 – 79.

[12] Dicks, W.; Dunwoody, M. J., *Groups acting on graphs*, Cambridge University Press, 1989.

[13] Dress, A.; Müller, T., *Decomposable functors and the exponential principle*, Adv. in Math. 129 (1997), 188 – 221.

[14] Euler, L., *Introductio in analysin infinitorum*, Marcum–Michaelem Bousquet, Lausannae, 1748.

[15] Gasper, G.; Rahman, M., *Basic hypergeometric series*, Encyclopedia of Mathematics and its Applications Vol. 35, Cambridge University Press, 1990.

[16] Gunning, R. C., *Lectures on modular forms*, Annals of Mathematics Studies No. 48, Princeton University Press, Princeton, New Jersey, 1962.

[17] Hall, M., *Subgroups of finite index in free groups*, Can. J. Math. 1 (1949), 187 – 190.

[18] Hall, P., *The Eulerian functions of a group*, Quart. J. Math. 7 (1936), 134 – 151.

[19] Harris, B.; Schoenfeld, L., *Asymptotic expansion for the coefficients of analytic functions*, Illinois J. Math. 12 (1968), 264 – 277.

[20] Hayman, W. K., *A generalization of Stirling's formula*, J. Reine u. Angew. Math. 196 (1956), 67 – 95.

[21] Karrass, A., Pietrowski, A. and Solitar, D., *Finite and infinite cyclic extensions of free groups*, J. Austral. Math. Soc. 16 (1973), 458 – 466.

[22] Kurosh, A., *Gruppentheorie I*, Akademie–Verlag, Berlin, 1970.

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

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

[25] Moser, L.; Wyman, M., *On the solutions of $x^d = 1$ in symmetric groups*, Can. J. Math. 7 (1955), 159–168.

[26] Müller, T., *Kombinatorische Aspekte endlich erzeugter virtuell freier Gruppen*, Ph. D. Thesis, Universität Frankfurt am Main, 1989.

[27] Müller, T., *Combinatorial aspects of finitely generated virtually free groups*, J. London Math. Soc. 44 (1991), 75–94.

[28] Müller, T., *Counting free subgroups of finite index*, Archiv d. Math. 59 (1992), 525–533.

[29] Müller, T., *Subgroup growth of free products*, Invent. Math. 126 (1996), 111–131.

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

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

[32] Müller, T., *Representations in finite wreath products and subgroup growth*, in preparation.

[33] Müller, T., *Poincaré's problem for free products*, in preparation.

[34] Müller, T.; Shareshian, J., *Enumerating representations in finite wreath products II: Explicit formulae*, submitted.

[35] Müller, T.; Shareshian, J., *Computing the Euler characteristic of the Quillen complex for certain groups*, in preparation.

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

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

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

[39] Pólya, G., *Über die Nullstellen sukzessiver Derivierten*, Math. Z. 12 (1922), 36 – 60.

[40] Quillen, D., *Homotopy properties of the poset of nontrivial p–subgroups of a group*, Adv. in Math. 28 (1978), 101 – 128.

[41] Rota, G.-C., *On the foundations of combinatorial theory*, I. Theory of Möbius functions, Z. Wahrscheinlichkeitstheorie u. verw. Geb. 2 (1964), 340 – 368.

[42] Serre, J.–P., *Cohomologie des groupes discrets*, Ann. Math. Studies 70, Princeton University Press, 1971.

[43] Serre, J.–P., *Trees*, Springer, Berlin, 1980.

[44] Stallings, J., *On torsion–free groups with infinitely many ends,* Annals of Math. 88 (1968), 312 – 334.

[45] Stothers, W. W., *The number of subgroups of given index in the modular group*, Proc. Royal Soc. Edinburgh 78A (1977), 105–112.

[46] Wilf, H., *The asymptotics of* $e^{P(z)}$ *and the number of elements of each order in* S_n, Bull. Amer. Math. Soc. 15 (1986), 228–232.

[47] Wohlfahrt, K., *Über einen Satz von Dey und die Modulgruppe,* Archiv d. Math. 29 (1977), 455 – 457.

[48] Wright, E. M., *A relationship between two sequences,* Proc. London Math. Soc. 17 (1967), 296–304.

[49] Wright, E. M., *Asymptotic relations between enumerative functions in graph theory,* Proc. London Math. Soc. 20 (1970), 558–572.

School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS
England