PARITY PATTERNS IN HECKE GROUPS AND FERMAT PRIMES

THOMAS W. MÜLLER

1. Introduction

For a group $\mathfrak{G}$ denote by $s_n(\mathfrak{G})$ the number of subgroups of index n in $\mathfrak{G}$. If $\mathfrak{G}$ is finitely generated or of finite (subgroup) rank, then $s_n(\mathfrak{G})$ is finite for all n. The present paper is concerned with the behaviour modulo 2 of the function $s_n(\mathfrak{G})$ and another arithmetic function counting free subgroups of finite index in the case when $\mathfrak{G}$ is a Hecke group. Rather surprisingly, it turns out that Fermat primes play an important special role in this context, a phenomenon hitherto unobserved in the arithmetic theory of Hecke groups, and, as a byproduct of our investigation, several new characterizations of Fermat primes are obtained.

The natural framework for our research is the theory of *subgroup growth* of finitely generated virtually free groups. The notion of subgroup growth, which has evolved over the last decade, brings together under a common conceptual roof investigations concerning arithmetic properties of the sequence $\{s_n(\mathfrak{G})\}_1^\infty$ or related subgroup counting functions and their connection with the algebraic structure of the group $\mathfrak{G}$. The original motivation for these studies comes from three sources: the notion of word growth and, more specifically, Gromov's characterization in [13] of finitely generated groups with polynomial word growth, the theory of rings of algebraic integers and their zeta functions, and the work of M. Hall and T. Radó in the late 1940's on Schreier systems and their associated subgroups in free groups; cf. [14], [15], and [16]. Most of the major developments up to 1992 are described in Lubotzky's Galway notes [19], [20], and the literature cited therein. More recent contributions include [7], [23], [24], [25], [27], [28], and [8].

Whereas for instance the growth behaviour and the asymptotics of the function $s_n(\mathfrak{G})$ tend to react fairly smoothly to variation of $\mathfrak{G}$, say, over a commensurability class, divisibility properties of $s_n(\mathfrak{G})$ are usually severely deformed if not completely destroyed in this process. The latter type of arithmetic structure appears to be rather subtle and peculiar to the particular group under investigation. This tendency (apart from considerable technical difficulties) may account for the fact that very little is known concerning divisibility properties of subgroup counting functions. Indeed, the only published results of major interest in the present context seem to be Stothers' formulae for the modular group. Before stating his results let us introduce some general notation. For a finitely generated group $\mathfrak{G}$ we define

$$\Pi(\mathfrak{G}) := \big\{n \in \mathbb{N} : \ s_n(\mathfrak{G}) \equiv 1 \bmod 2\big\}.$$

Moreover, for $\mathfrak{G}$ a finitely generated virtually free group, let

$$\Pi^*(\mathfrak{G}) := \big\{\lambda \in \mathbb{N} : \ b_\lambda(\mathfrak{G}) \equiv 1 \bmod 2\big\}.$$

Here, $b_\lambda(\mathfrak{G})$ is the number of free subgroups in $\mathfrak{G}$ of index $\lambda m_{\mathfrak{G}}$, and $m_{\mathfrak{G}}$ denotes the least common multiple of the orders of the finite subgroups in $\mathfrak{G}$. We call $\Pi(\mathfrak{G})$ and $\Pi^*(\mathfrak{G})$ the *parity pattern* respectively *free parity pattern* of the group $\mathfrak{G}$. In this notation the main result of Stothers [34] is that

$$\Pi(PSL(2,\mathbb{Z})) = \left\{2^{\sigma+1}-3\right\}_1^\infty \cup 2\left\{2^{\sigma+1}-3\right\}_1^\infty. \tag{1}$$

This striking result, which had been conjectured for some time on the basis of numerical evidence, has, for more than 20 years, stood out as an indication that a fascinating chapter of subgroup arithmetic might still be awaiting its discovery. In the course of his proof Stothers also shows that

$$\Pi^*(PSL(2,\mathbb{Z})) = \left\{2^{\sigma}-1\right\}_1^\infty. \tag{2}$$

The latter pattern has been shown to occur for a larger class of virtually free groups of free rank 2, including free products $\mathfrak{G} = G_1 *_S G_2$ of two finite groups G_i with an amalgamated subgroup S of odd cardinality, whose indices $(G_i : S)$ satisfy $\{(G_1 : S), (G_2 : S)\} = \{2,3\}$ or $= \{2,4\}$; cf. [22, Prop. 6]. [1]

For an integer $q \geq 3$ let $\mathfrak{H}(q)$ be the Hecke group corresponding to q, i.e., the group of linear fractional transformations generated by the transformations $\tau' = -1/\tau$ and $\tau' = \tau + 2\cos(\pi/q)$. We have $\mathfrak{H}(3) = \mathrm{PSL}(2,\mathbb{Z})$, and in general $\mathfrak{H}(q)$ is a subgroup of $\mathrm{PSL}(2,R)$, where R is the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_q + \zeta_q^{-1})$ with $\zeta_q = \mathrm{e}^{i\pi/q}$. The precise structure of the matrices entering into this representation of $\mathfrak{H}(q)$ is not in general known. As an abstract group, $\mathfrak{H}(q)$ is the free product of a cyclic group of order 2 and a cyclic group of order q; in particular, $\mathfrak{H}(q)$ is virtually free. The purpose of this paper is to investigate the parity patterns $\Pi(\mathfrak{H}(q))$ and $\Pi^*(\mathfrak{H}(q))$ for $q \geq 3$.

There are several a priori reasons to suspect that Hecke groups might prove to be an interesting and fruitful class of groups to study with regard to their parity patterns and similar number–theoretic properties: (i) The groups $\mathfrak{H}(q)$ form what is probably the most natural generalization of the modular group, sharing the latter's central position in large parts of mathematics, in particular its close ties with number theory. (ii) In 1998, building on results obtained in [21], an analogue of Stothers' formula (1) for $q = 5$ was discovered by the author, namely

$$\Pi(\mathfrak{H}(5)) = \left\{\frac{2^{2\sigma+1}-5}{3}\right\}_1^\infty \cup 2\left\{\frac{2^{2\sigma+1}-5}{3}\right\}_1^\infty; \tag{3}$$

cf. [29].[2] (iii) According to a result of Grady and Newman a free product $\mathfrak{G}$ of finitely many cyclic groups of prime order containing at least four copies of the cyclic group of order 2 in its free decompositon satisfies $\Pi(\mathfrak{G}) = \mathbb{N}$; cf. [11, Theorem 1]. In the same paper Grady and Newman conjecture that two free factors C_2 should already suffice to ensure the same conclusion. This conjecture, if true, would place Hecke groups within a rather tight borderline region, which might well deserve further study. The more specific conjecture made in [10] to the effect that a free product of two or more copies of the

---

[1] The free rank $\mu(\mathfrak{G})$ of a finitely generated virtually free group $\mathfrak{G}$ is defined as the rank of a free subgroup of index $m_{\mathfrak{G}}$ in $\mathfrak{G}$. See Section 2.1 below.

[2] Recently, I have been informed by W. Imrich, that he and his doctoral student Yao have also obtained formula (3) by a somewhat different method.

cyclic group of order 2 should have all its subgroup numbers odd, follows immediately from one of our results (see Proposition F below). (iv) So far, parity patterns have only been studied for groups of free rank at most 3, and there are some indications that for fixed free rank only a very small number of non–trivial patterns arise. The fact that the free rank $\mu(\mathfrak{H}(q))$ becomes unbounded as $q \to \infty$, while accounting for technical difficulties well beyond the scope of any previously known method of investigation, adds considerably to the interest of Hecke groups as a class of “test samples” with regard to this type of arithmetic structure.

We now turn to the main results of this paper. Somewhat surprisingly, formulae (1)–(3) do not generalize to all Hecke groups. Instead, there exist canonical (and maximal) generalizations of Stothers' formulae (1) and (2), each characterizing a particular subclass of Hecke groups (see Theorems A and B below). Moreover, both these subclasses essentially correspond to certain “arithmetic singularities”, outside of which the subgroup counting function under investigation displays a peculiar type of fractal behaviour, thus ruling out the possibility of describing the associated parity pattern by a closed formula à la Stothers. For an integer $q \geq 3$ define

$$\Lambda_q^* := \left\{ \frac{\mu_q^\sigma - 1}{\mu_q - 1} : \ \sigma = 1, 2, \dots \right\},$$

i.e., Λ_q^* is the set of partial sums of the geometric series generated by the free rank $\mu_q := \mu(\mathfrak{H}(q))$ of $\mathfrak{H}(q)$. Our first main result characterizes those Hecke groups whose free parity pattern canonically generalizes the pattern found by Stothers for the modular group.

Theorem A. *Let $q \geq 3$ be an integer. Then the following assertions are equivalent:*

(i) $\Pi^*(\mathfrak{H}(q)) = \Lambda_q^*$.

(ii) $b_\lambda(\mathfrak{H}(q)) \equiv 0 \ (2)$ *for* $2 \leq \lambda \leq \mu_q$.

(iii) q *or* $q-1$ *is a 2–power.*

As is well known, Fermat primes, i.e., prime numbers of the form $2^{2^\lambda} + 1$ with $\lambda \geq 0$, satisfy (or can even be characterized by) a number of curious regularity conditions; for instance, according to Gauss, [3] a regular p–gon ($p > 2$ a prime) can be constructed by compass and ruler if and only if p is a Fermat prime. By specializing Theorem A to the case when q is a prime number we obtain a new such characterization.

Corollary A$'$. *Let $q > 2$ be a prime. Then q is a Fermat prime if and only if* $\Pi^*(\mathfrak{H}(q)) = \Lambda_q^*$.

The connection with Fermat primes becomes even more striking when turning to the patterns $\Pi(\mathfrak{H}(q))$. For $q \geq 3$ define

$$\Lambda_q := \left\{ \frac{2(q-1)^\sigma - q}{q-2} \right\}_1^\infty,$$

i.e., Λ_q is the set of partial sums of the series $1 + 2\sum_{\sigma=1}^\infty (q-1)^\sigma$.

[3] Disquisitiones arithmeticae, § 366.

Theorem B. (a) *For even $q > 2$ we have $\Pi(\mathfrak{H}(q)) = \mathbb{N}$.*

(b) *Let $q \geq 3$ be an odd integer. Then the following assertions are equivalent:*

(i) $\Pi(\mathfrak{H}(q)) = \Lambda_q \cup 2\,\Lambda_q$.

(ii) $s_n(\mathfrak{H}(q)) \equiv 0\ (2)$ *for n odd and $n \in [2q(q-1)] - \{1, 2q-1\}$.*

(iii) *q is a Fermat prime.*

We also establish certain general properties of $\Pi^*(\mathfrak{H}(q))$ and $\Pi(\mathfrak{H}(q))$, a number of which are summarized in the next two results.

Theorem C. (a) *For every $q \geq 3$ the set $\Pi^*(\mathfrak{H}(q))$ is infinite.*
(b) *Let $q_1, q_2 \geq 3$ be integers. Then we have $\Pi^*(\mathfrak{H}(q_1)) = \Pi^*(\mathfrak{H}(q_2))$ if and only if $\mu_{q_1} = \mu_{q_2}$.*
(c) *Let $\alpha^* \geq 2$ be an integer. Then 1 and α^* are the first two entries of a free parity pattern of some Hecke group if and only if $\alpha^* - 1$ is a 2–power.*

Theorem D. (a) *For every odd $q \geq 3$ the set $\Pi(\mathfrak{H}(q))$ is infinite.*
(b) *Let $q_1, q_2 \geq 3$ be odd integers, and suppose that $\Pi(\mathfrak{H}(q_1)) = \Pi(\mathfrak{H}(q_2))$. Then we have $q_1 = q_2$.*
(c) *For odd $q \geq 3$ the first entries of $\Pi(\mathfrak{H}(q))$ are $1, 2$, and $2p(q) - 1$, where $p(q)$ denotes the smallest prime divisor of q.*

Furthermore, we obtain fairly explicit descriptions of $\Pi^*(\mathfrak{H}(q))$ and $\Pi(\mathfrak{H}(q))$ for arbitrary q. We quote the result for the free parity pattern; for $\Pi(\mathfrak{H}(q))$ and odd $q \geq 3$ a similar but slightly more complicated formula holds true.[4] Call a sequence $\underline{\alpha} = \{\alpha_i\}_0^\infty \in \mathbb{N}_0^{\mathbb{N}_0}$ *finitary*, if there exists some $\mu \in \mathbb{N}_0$ such that $\alpha_i = 0$ for all $i > \mu$. The *norm* $||\underline{\alpha}||$ of a finitary sequence $\underline{\alpha}$ is defined as $||\underline{\alpha}|| = \sum_{i \geq 0} \alpha_i$. Let

$$\mathcal{A} := \Big\{ \underline{\alpha} \in \mathbb{N}_0^{\mathbb{N}_0} :\ \underline{\alpha} \text{ is finitary and } \alpha_0 = 1 \Big\}.$$

Theorem E. *For every $q \geq 3$ we have*

$$\Pi^*(\mathfrak{H}(q)) = \left\{ \lambda \in \mathbb{N} :\ \sum_{\substack{\underline{\alpha} \in \mathcal{A} \\ ||\underline{\alpha}|| = \lambda}} \prod_{i=0}^{\infty} \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} \equiv 1 \bmod 2 \right\}.$$

Sections 2–4 of the present paper are concerned with the free parity patterns $\Pi^*(\mathfrak{H}(q))$. In Section 2, building on results of [22], we derive a new recurrence relation for the function $b_\lambda(\mathfrak{G})$, which is not of Hall type and is, at least in principle, fairly well adapted for studying divisibility properties, but rather complicated and awkward to handle. However, a careful analysis of this recursion, undertaken in Section 3, leads to the much simpler identity

$$X_q^*(z) = 1 + z\left(X_q^*(z)\right)^{\mu_q} \tag{4}$$

for the mod 2 projection $X_q^*(z) \in GF(2)[[z]]$ of the generating function $1 + \sum_{\lambda=1}^\infty b_\lambda(\mathfrak{H}(q)) z^\lambda$, and our results for the patterns $\Pi^*(\mathfrak{H}(q))$ follow from a thorough discussion of (4). The analysis of the patterns $\Pi(\mathfrak{H}(q))$ is considerably more involved. Instead of working

[4] Cf. Section 7.2, Theorem 12.

directly with $\mathfrak{H}(q)$ we first consider the group $\widetilde{\mathfrak{H}}(q) := C_q * C_q$ which embeds in the corresponding Hecke group as a subgroup of index 2. Indeed, if $\mathfrak{H}(q) = \langle \sigma, \tau | \sigma^2 = \tau^q = 1\rangle$, then the subgroup generated by τ and τ^σ is isomorphic to $\widetilde{\mathfrak{H}}(q)$ with transversal $\{1, \sigma\}$, so that $\mathfrak{H}(q)$ is in fact a split extension of the group $\widetilde{\mathfrak{H}}(q)$ by C_2. The connection between the parity patterns of these two groups is given by the following general observation.

Proposition F. *Let $\mathfrak{G}$ be a group containing only finitely many subgroups of index n for every positive integer n, and let $\mathfrak{H}$ be a subgroup of index 2 in $\mathfrak{G}$. Then*

$$\Pi(\mathfrak{G}) = \Big(\Pi(\mathfrak{H}) \,\cap\, (\mathbb{N} - 2\mathbb{N})\Big) \,\cup\, 2\,\Pi(\mathfrak{H}). \tag{5}$$

This rather surprising relationship allows us in particular to translate results concerning the parity patterns of the groups $\widetilde{\mathfrak{H}}(q)$ into results for the patterns $\Pi(\mathfrak{H}(q))$. It also bears on the conjecture of Grady and Newman concerning groups of the form $\mathfrak{G} = C_2 * \ldots * C_2$ mentioned earlier in this introduction. At first sight, replacing the investigation of the parity pattern $\Pi(\mathfrak{H}(q))$ by the corresponding problem for the group $\widetilde{\mathfrak{H}}(q)$ might not strike one as a particularly promising reduction, since for $q > 5$ both groups have so far entirely resisted all attempts at such an analysis, due to the enormous complexity of the arithmetic functions involved, which becomes uncontrollable as $q \to \infty$. A breakthrough for the groups $\widetilde{\mathfrak{H}}(q)$ – and hence via (5) for Hecke groups – is made possible by (i) divising an approach concentrating the main complexity of the problem in the series

$$\mathcal{R}_q^{\mu,\nu}(z) := \frac{d^\nu}{dz^\nu}\Big\{\sum_{n=0}^{\infty} h_n(q)\, h_{n+\mu}(q)\, z^n/n!\Big\}\Big/\Big\{\sum_{n=0}^{\infty} h_n^2(q)\, z^n/n!\Big\},$$

where $h_n(q) := |\operatorname{Hom}(C_q, S_n)|$, (ii) showing that for $q \geq 3$, $\mu \geq 0$, and $\nu \geq 0$ the series $\mathcal{R}_q^{\mu,\nu}(z)$ are in fact *integral* power series, and (iii) the fact that in the critical equation (45) governing the generating function $\sum_{n=0}^{\infty} s_{n+1}(\widetilde{\mathfrak{H}}(q))z^n$ the series $\mathcal{R}_q^{\mu,\nu}(z)$, apart from shift factors, always occur with even coefficient, and thus, given (ii), can be ignored modulo 2 (this is the advantage of working with the groups $\widetilde{\mathfrak{H}}(q)$). It is remarkable that, while an exact computation of the remainder terms $\mathcal{R}_q^{\mu,\nu}(z)$ (which all previous attempts have, at least implicitly, aimed at) appears entirely out of reach for large q, their mere integrality can, by a fairly subtle argument occupying the whole of Section 6, be established for arbitrary q. As a consequence of these developments we obtain the differential equation

$$\widetilde{X}_q(z) = \sum_{d|q}\sum_{\mu\geq 0} z^{2d-3}\left(\widetilde{X}_q'(z)\right)^{\mu}\left(\widetilde{X}_q(z)\right)^{d-2(\mu+1)}\left[\binom{d-1}{2\mu} z\,\widetilde{X}_q(z) \,+\, (d-1)\binom{d-2}{2\mu}\right] \tag{6}$$

for the mod 2 projection $\widetilde{X}_q(z)$ of the generating function $\sum_{n=0}^{\infty} s_{n+1}(\widetilde{\mathfrak{H}}(q))\, z^n$. A detailed analysis of equation (6) then leads to a rather complete set of results for the parity patterns $\Pi(\widetilde{\mathfrak{H}}(q))$, which are translated into results concerning the patterns $\Pi(\mathfrak{H}(q))$ in Section 7, following the proof of Proposition F.

2. Some preliminaries concerning virtually free groups

2.1. **The structure theorem and some invariants.** Let $\mathfrak{G}$ be a finitely generated virtually free group and denote by $m_{\mathfrak{G}}$ the least common multiple of the orders of the finite subgroups in $\mathfrak{G}$. By Stallings' structure theorem on groups with infinitely many ends and the subsequent work of Karrass, Pietrowski, and Solitar, $\mathfrak{G}$ can be presented as the fundamental group of a finite graph of groups $(\mathfrak{G}(-), Y)$ in the sense of Bass and Serre with finite vertex groups $\mathfrak{G}(v)$; cf. [33] and [18], or [5, Sect. IV.1.9]. The fact that, conversely, the fundamental group of a finite graph of finite groups is always virtually free of finite rank is more elementary, and can be found for instance in [31, Sect. II.2.6]. It follows in particular from this characterisation and the universal covering construction in the category of graphs of groups that a torsion–free subgroup of a finitely generated virtually free group is in fact free (which was the original contribution of Stallings' work to the structure theory of virtually free groups).

If $\mathfrak{G}'$ is a free subgroup of finite index in $\mathfrak{G}$ then, following an idea of Wall, one defines the rational Euler characteristic $\chi(\mathfrak{G})$ of $\mathfrak{G}$ as

$$\chi(\mathfrak{G}) = -\frac{\mathrm{rk}(\mathfrak{G}') - 1}{(\mathfrak{G} : \mathfrak{G}')}. \tag{7}$$

This is well–defined in view of Schreier's theorem [30], and if $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-), Y)$ is a decomposition of $\mathfrak{G}$ in terms of a graph of groups, then we have

$$\chi(\mathfrak{G}) = \sum_{v \in V(Y)} \frac{1}{|\mathfrak{G}(v)|} - \sum_{e \in E(Y)} \frac{1}{|\mathfrak{G}(e)|}, \tag{8}$$

where $V(Y)$ and $E(Y)$ denote respectively the set of vertices and (geometric) edges of Y.The latter formula reflects the fact that in our situation the Euler characteristic in the sense of Wall coincides with the equivariant Euler characteristic $\chi_T(\mathfrak{G})$ of $\mathfrak{G}$ relative to the tree T canonically associated with $\mathfrak{G}$ in the sense of Bass and Serre; cf. [1, Chap. IX, Prop. 7.3] or [32, Prop. 14]. Define the (free) rank $\mu(\mathfrak{G})$ of $\mathfrak{G}$ to be the rank of a free subgroup of index $m_{\mathfrak{G}}$ in $\mathfrak{G}$. The existence of such a subgroup follows from [31, Lemmas 8 and 10] or formulae (11) and (12) below. Observe that, in view of (7), $\mu(\mathfrak{G})$ is connected with the Euler characteristic of $\mathfrak{G}$ via

$$\mu(\mathfrak{G}) + m_{\mathfrak{G}}\chi(\mathfrak{G}) = 1, \tag{9}$$

which shows in particular that $\mu(\mathfrak{G})$ is well–defined.

The type $\tau(\mathfrak{G})$ of a finitely generated virtually free group $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-), Y)$ is defined as the tuple

$$\tau(\mathfrak{G}) = \big(m_{\mathfrak{G}}; \zeta_1(\mathfrak{G}), \ldots, \zeta_\kappa(\mathfrak{G}), \ldots, \zeta_{m_{\mathfrak{G}}}(\mathfrak{G})\big),$$

where the $\zeta_\kappa(\mathfrak{G})$ are integers indexed by the divisors of $m_{\mathfrak{G}}$, given by

$$\zeta_\kappa(\mathfrak{G}) = \Big|\Big\{e \in E(Y) : \, |\mathfrak{G}(e)| \,\Big|\, \kappa\Big\}\Big| - \Big|\Big\{v \in V(Y) : \, |\mathfrak{G}(v)| \,\Big|\, \kappa\Big\}\Big|.$$

It can be shown that the type $\tau(\mathfrak{G})$ is in fact an invariant of the group $\mathfrak{G}$, i.e. independent of the particular decomposition of $\mathfrak{G}$ in terms of a graph of groups $(\mathfrak{G}(-), Y)$, and that two virtually free groups $\mathfrak{G}_1$ and $\mathfrak{G}_2$ contain the same number of free subgroups of index n for each $n \in \mathbb{N}$ if and only if $\tau(\mathfrak{G}_1) = \tau(\mathfrak{G}_2)$; cf. [22, Theorem 2]. Note that as a consequence of (8) the Euler characteristic of $\mathfrak{G}$ can be expressed in terms of the type $\tau(\mathfrak{G})$ via

$$\chi(\mathfrak{G}) = -m_{\mathfrak{G}}^{-1} \sum_{\kappa \mid m_{\mathfrak{G}}} \varphi(m_{\mathfrak{G}}/\kappa)\, \zeta_\kappa(\mathfrak{G}), \tag{10}$$

where φ is Euler's function. It follows in particular that if two virtually free groups have the same number of free index n subgroups for every n, then their Euler characteristics must coincide.

2.2. **The functions $a_\lambda(\mathfrak{G})$ and $b_\lambda(\mathfrak{G})$.** The total information on the number of free subgroups of given finite index in a finitely generated virtually free group $\mathfrak{G}$ is concentrated in the constant $m_{\mathfrak{G}}$ and the function $b(\mathfrak{G}) : \mathbb{N} \to \mathbb{N}$ given by

$$b_\lambda(\mathfrak{G}) = \text{number of free subgroups of index } \lambda m_{\mathfrak{G}} \text{ in } \mathfrak{G}.$$

Our approach to the function $b_\lambda(\mathfrak{G})$ is to relate it to another arithmetic function $a_\lambda(\mathfrak{G})$ which turns out to be easier to compute. Define a torsion–free $\mathfrak{G}$–action on a set Ω to be a $\mathfrak{G}$–action on Ω which is free when restricted to finite subgroups. For a finite set Ω to admit a torsion–free $\mathfrak{G}$–action it is necessary and sufficient that $|\Omega|$ be divisible by $m_{\mathfrak{G}}$. For $\lambda \in \mathbb{N}_0$ define $a_\lambda(\mathfrak{G})$ by the condition that

$$(\lambda m_{\mathfrak{G}})!\, a_\lambda(\mathfrak{G}) = \text{number of torsion–free } \mathfrak{G}\text{–actions on a set with } \lambda m_{\mathfrak{G}} \text{ elements},$$

in particular $a_0(\mathfrak{G}) = 1$. Then the arithmetic functions $a_\lambda(\mathfrak{G})$ and $b_\lambda(\mathfrak{G})$ are related via the transformation formula[5]

$$\sum_{\mu=1}^{\lambda} a_{\lambda-\mu}(\mathfrak{G})\, b_\mu(\mathfrak{G}) = m_{\mathfrak{G}}\, \lambda\, a_\lambda(\mathfrak{G}), \quad \lambda \geq 1. \tag{11}$$

Moreover, a careful analysis of the universal mapping property associated with the presentation $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-), Y)$ of $\mathfrak{G}$ in terms of a graph of groups $(\mathfrak{G}(-), Y)$ leads to the explicit formula

$$a_\lambda(\mathfrak{G}) = \frac{\prod\limits_{e \in E(Y)} \Big[(\lambda m_{\mathfrak{G}}/|\mathfrak{G}(e)|)!\, |\mathfrak{G}(e)|^{\lambda m_{\mathfrak{G}}/|\mathfrak{G}(e)|}\Big]}{\prod\limits_{v \in V(Y)} \Big[(\lambda m_{\mathfrak{G}}/|\mathfrak{G}(v)|)!\, |\mathfrak{G}(v)|^{\lambda m_{\mathfrak{G}}/|\mathfrak{G}(v)|}\Big]}, \quad \lambda \geq 0 \tag{12}$$

for $a_\lambda(\mathfrak{G})$; compare [22, Prop. 3]. From this formula it can be deduced that the sequence $a_\lambda(\mathfrak{G})$ is of hypergeometric type and that the generating function $\alpha_{\mathfrak{G}}(z) := \sum_{\lambda=0}^\infty a_\lambda(\mathfrak{G}) z^\lambda$ satisfies a homogeneous linear differential equation

$$A_0(\mathfrak{G})\, \alpha_{\mathfrak{G}}(z) \;+\; (A_1(\mathfrak{G})\, z - m_{\mathfrak{G}})\, \alpha'_{\mathfrak{G}}(z) \;+\; \sum_{\mu=2}^{\mu(\mathfrak{G})} A_\mu(\mathfrak{G})\, z^\mu\, \alpha_{\mathfrak{G}}^{(\mu)}(z) = 0 \tag{13}$$

[5] See for instance [22, Cor. 1].

of order $\mu(\mathfrak{G})$ with integral coefficients

$$A_\mu(\mathfrak{G}) = \frac{1}{\mu!}\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j} m_{\mathfrak{G}}\,(j+1)\prod_{\kappa\mid m_{\mathfrak{G}}}\prod_{\substack{1\leq k\leq m_{\mathfrak{G}}\\ (m_{\mathfrak{G}},k)=\kappa}}(jm_{\mathfrak{G}}+k)^{\zeta_\kappa(\mathfrak{G})},\quad 0\leq\mu\leq\mu(\mathfrak{G}); \tag{14}$$

cf. [22, Prop. 5].

2.3. **A recurrence relation for $b_\lambda(\mathfrak{G})$.** Inserting formula (12) into (11) yields a recursive description of the arithmetic function $b_\lambda(\mathfrak{G})$ attached to a finitely generated virtually free group $\mathfrak{G}$. However, formulae obtained in this way (referred to as being of Hall type) usually turn out to be quite unsatisfactory when dealing with number–theoretic aspects of the sequence $b_\lambda(\mathfrak{G})$ such as divisibility properties. Instead, we will derive a recurrence relation for $b_\lambda(\mathfrak{G})$ which differs considerably in form from (11) and is rather well adapted for studying divisibility properties of the function $b_\lambda(\mathfrak{G})$. The following result will be the starting point of our present investigations.

Proposition 1. *Let $\mathfrak{G}$ be a finitely generated virtually free group. Then the function $b_\lambda(\mathfrak{G})$ satisfies the recursion*

$$b_{\lambda+1}(\mathfrak{G}) \;=\; \sum_{\mu=1}^{\mu(\mathfrak{G})}\;\sum_{\substack{\lambda_1,\dots,\lambda_\mu>0\\ \lambda_1+\cdots+\lambda_\mu=\lambda}}(\mu!\,m_{\mathfrak{G}}^{\mu})^{-1}\,\mathcal{B}_\mu^{(\mathfrak{G})}(\lambda_1,\dots,\lambda_\mu)\,\prod_{j=1}^{\mu}b_{\lambda_j}(\mathfrak{G}) \qquad (\lambda\geq 1,\; b_1(\mathfrak{G})=A_0(\mathfrak{G})) \tag{15}$$

with coefficients

$$\mathcal{B}_\mu^{(\mathfrak{G})}(\lambda_1,\dots,\lambda_\mu) := \sum_{\nu=\mu}^{\mu(\mathfrak{G})}A_\nu(\mathfrak{G})\,B_{\mu,\nu}(\lambda_1,\dots,\lambda_\mu),$$

where

$$B_{\mu,\nu}(\lambda_1,\dots,\lambda_\mu) := \nu!\sum_{\substack{\nu_1,\dots,\nu_\mu\geq 0\\ \nu_1+\cdots+\nu_\mu=\nu-\mu}}\;\prod_{j=1}^{\mu}\left[\binom{\lambda_j-1}{\nu_j}/(\nu_j+1)\right]$$

and $A_\nu(\mathfrak{G})$ is as in (14).

Proof. Introduce the generating function

$$\beta_{\mathfrak{G}}(z) := \sum_{\lambda=0}^{\infty}b_{\lambda+1}(\mathfrak{G})\,z^\lambda.$$

Then, in view of equation (11), $\beta_{\mathfrak{G}}(z)$ is related to $\alpha_{\mathfrak{G}}(z)$ via the identity

$$\beta_{\mathfrak{G}}(z) = m_{\mathfrak{G}}\,\frac{d}{dz}\big(\log\,\alpha_{\mathfrak{G}}(z)\big). \tag{16}$$

We will use Bell's formula[6]

$$\frac{d^\mu}{dz^\mu} f(g(z)) = \sum_{\pi \vdash \mu} \frac{\mu!}{\prod_{j=1}^\infty \pi_j!} \left[\prod_{j=1}^\infty \left(\frac{g^{(j)}(z)}{j!}\right)^{\pi_j}\right] f^{(\|\pi\|)}(g(z)) \tag{17}$$

for the derivatives of a composite function to calculate the higher derivatives of $\alpha_{\mathfrak{G}}(z) = \exp(m_{\mathfrak{G}}^{-1} \int \beta_{\mathfrak{G}}(z)\,dz)$. Applying (17) with $f(t) = \mathrm{e}^t$ and $g(z) = m_{\mathfrak{G}}^{-1} \int \beta_{\mathfrak{G}}(z)\,dz$ we find after some routine manipulations that

$$\alpha_{\mathfrak{G}}^{(\mu)}(z) = \mu!\,\alpha_{\mathfrak{G}}(z) \sum_{\nu=1}^{\mu} \sum_{\substack{\mu_1,\dots,\mu_\nu>0\\ \mu_1+\cdots+\mu_\nu=\mu}} (\nu!\,m_{\mathfrak{G}}^\nu)^{-1} \prod_{j=1}^{\nu} \frac{\beta_{\mathfrak{G}}^{(\mu_j-1)}(z)}{\mu_j!}, \quad \mu \geq 1.$$

Combining these identities for $1 \leq \mu \leq \mu(\mathfrak{G})$ with (13) we obtain for $\beta_{\mathfrak{G}}(z)$ the differential equation

$$\beta_{\mathfrak{G}}(z) = A_0(\mathfrak{G}) + \sum_{\mu=1}^{\mu(\mathfrak{G})} \sum_{\nu=1}^{\mu} \sum_{\substack{\mu_1,\dots,\mu_\nu>0\\ \mu_1+\cdots+\mu_\nu=\mu}} \binom{\mu}{\mu_1,\dots,\mu_\nu} (\nu!\,m_{\mathfrak{G}}^\nu)^{-1} A_\mu(\mathfrak{G})\, z^\mu \prod_{j=1}^{\nu} \beta_{\mathfrak{G}}^{(\mu_j-1)}(z) \tag{18}$$

with $A_\mu(\mathfrak{G})$ as in (14). Our claim (15) follows now by comparing coefficients in (18). □

Remark 1. *Since the numbers $A_\nu(\mathfrak{G})$ as well as the $B_{\mu,\nu}(\lambda_1,\dots,\lambda_\mu)$ are integral, so are the numbers $\mathcal{B}_\mu^{(\mathfrak{G})}(\lambda_1,\dots,\lambda_\mu)$, and the recursion (15) comes rather close to having all its coefficients $(\mu!\,m_{\mathfrak{G}}^\mu)^{-1}\,\mathcal{B}_\mu^{(\mathfrak{G})}(\lambda_1,\dots,\lambda_\mu)$ in $\mathbb{Z}$. However, if $\mathfrak{G} = F_r$ is the free group of rank r, then $m_{\mathfrak{G}} = 1$ and $A_\nu(\mathfrak{G}) = S(r+1,\nu+1)$ is a Stirling number of the second kind, and if $r \geq 2$ the coefficient for $\mu = r-1$ turns out to be*

$$\big((r-1)!\big)^{-1}\,\mathcal{B}_{r-1}^{(F_r)}(\lambda_1,\dots,\lambda_{r-1}) = \frac{r(\lambda+2)}{2},$$

which is not in general integral. Also, for $\mathfrak{G} = F_4$, the coefficients for $\mu = 2$ are

$$\frac{\mathcal{B}_2^{(F_4)}(\lambda_1,\lambda_2)}{2} = 2(\lambda+1)(\lambda+2) - (\lambda_1+1)(\lambda_2+1) + 5,$$

which depends on the variables λ_1 and λ_2, and not only on their sum λ.

3. A recursive description of the function $\chi_q^*(\lambda)$

Write $\chi_q^*(\lambda)$ for $b_q(\lambda) := b_\lambda(\mathfrak{H}(q))$ considered modulo 2, so that χ_q^* is nothing but the characteristic function of the set $\Pi_q^* := \Pi^*(\mathfrak{H}(q)) \subseteq \mathbb{N}$. The purpose of this section is to establish a recursive description of the function $\chi_q^*(\lambda)$, which in turn will be used in the next section to prove our main results concerning the parity patterns Π_q^*.

[6] By a partition π we mean any sequence $\pi = \{\pi_j\}_1^\infty$ of non–negative integers, such that $\pi_j = 0$ for all but finitely many j. $|\pi| = \sum_{j=1}^\infty j\,\pi_j$ is called the weight of π, and $\|\pi\| = \sum_{j=1}^\infty \pi_j$ is the norm or length of the partition π. If $|\pi| = 0$, π is called the empty partition, otherwise π is non–empty. As usual, we also write $\pi \vdash \mu$ for $|\pi| = \mu$, and say that π is a partition of μ.

3.1. **Some computations and a lemma.** Concerning the invariants considered in the last section we find for $\mathfrak{G} = \mathfrak{H}(q)$ the following.

$$m_q := m_{\mathfrak{H}(q)} = \begin{cases} q, & q \text{ even} \\ 2q, & q \text{ odd}, \end{cases} \tag{19}$$

in particular, m_q is always even. Indeed, if $\mathfrak{G}$ is any finitely generated virtually free group and $(\mathfrak{G}(-), Y)$ is a Stallings decomposition for $\mathfrak{G}$, then we have

$$m_{\mathfrak{G}} = \big[|\mathfrak{G}(v)| : \, v \in V(Y)\big],$$

i.e., $m_{\mathfrak{G}}$ coincides with the least common multiple of the orders of the vertex groups in this decomposition. This follows from the universal covering construction and the fact that a finite group has to fix a vertex when acting on a tree.

For $\kappa \mid m_q$,

$$\zeta_\kappa^{(q)} := \zeta_\kappa(\mathfrak{H}(q)) = \begin{cases} 1, & 2 \nmid \kappa \text{ and } \kappa < q \\ -1, & \kappa = m_q \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

By (8), (9), and (19) we have

$$\chi(\mathfrak{H}(q)) = -\frac{q-2}{2q}$$

and

$$\mu_q := \mu(\mathfrak{H}(q)) = \begin{cases} q-1, & q \text{ odd} \\ q/2, & q \text{ even.} \end{cases}$$

Write $A_\mu^{(q)}$ for $A_\mu(\mathfrak{H}(q))$. The following result describes an important divisibility property of the $A_\mu^{(q)}$.

Lemma 1. *For $0 \leq \mu \leq \mu_q$ the integer $A_\mu^{(q)}$ is divisible by m_q^μ, and*

$$m_q^{-\mu} A_\mu^{(q)} \equiv \binom{\mu_q}{\mu} \mod 2.$$

Proof. Denote by K_q the set of all integers k satisfying $1 \leq k \leq m_q$ and $2 \nmid (k, m_q) < q$. This set has

$$\sum_{\substack{\kappa \mid q \\ 2 \nmid \kappa < q}} \varphi(m_q/\kappa) = \mu_q$$

elements. Here, we have used (20) plus equations (9) and (10) to evaluate the left–hand sum. We have

$$A_\mu^{(q)} = \frac{1}{\mu!} \sum_{j=0}^{\mu} (-1)^{\mu-j} \binom{\mu}{j} \prod_{k \in K_q} (k + j\, m_q) \tag{21}$$

and

$$\prod_{k\in K_q}(k+j\,m_q)=\prod_{k\in K_q}k\;+\;\sum_{\nu=1}^{\mu_q}(j\,m_q)^\nu\left(\prod_{k\in K_q}k\right)\left(\sum_{\substack{k_1,\dots,k_\nu\in K_q\\ k_1<\dots<k_\nu}}\frac{1}{k_1\dots k_\nu}\right). \tag{22}$$

Since

$$A_0^{(q)}=\prod_{k\in K_q}k\equiv 1\quad(2),$$

we may assume that $\mu>0$. Inserting (22) into (21) and using the facts that

$$\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j}=0\quad(\mu>0),$$

and that

$$\frac{1}{\mu!}\sum_{j=1}^{\mu}(-1)^{\mu-j}\binom{\mu}{j}j^\nu=S(\nu,\mu)\quad(\mu,\nu>0)$$

is a Stirling number of the second kind, we find that for $\mu>0$

$$A_\mu^{(q)}=m_q^\mu\left[\left(\prod_{k\in K_q}k\right)\left(\sum_{\substack{k_1,\dots,k_\mu\in K_q\\ k_1<\dots<k_\mu}}\frac{1}{k_1\dots k_\mu}\right)\;+\right.$$

$$\left.\sum_{\nu=\mu+1}^{\mu_q}m_q^{\nu-\mu}\,S(\nu,\mu)\left(\prod_{k\in K_q}k\right)\left(\sum_{\substack{k_1,\dots,k_\nu\in K_q\\ k_1<\dots<k_\nu}}\frac{1}{k_1\dots k_\nu}\right)\right].$$

This shows that $A_\mu^{(q)}$ is divisible by m_q^μ for all μ with $0<\mu\le\mu_q$, and that for each such μ

$$m_q^{-\mu}\,A_\mu^{(q)}\equiv\left(\prod_{k\in K_q}k\right)\left(\sum_{\substack{k_1,\dots,k_\mu\in K_q\\ k_1<\dots<k_\mu}}\frac{1}{k_1\dots k_\mu}\right)\quad\text{mod }2.$$

The right–hand side of the latter congruence is a sum of $\binom{\mu_q}{\mu}$ odd integers, whence the lemma. □

3.2. **The function $\chi_q^*(\lambda)$.** We shall require one further piece of preparation.[7]

Lemma 2. *Let $\pi=\{\pi_j\}_1^\infty$ be a partition. Then we have*

$$\nu_2\left(\prod_{j=1}^{\infty}j^{\pi_j}\right)\le\nu_2((2(|\pi|-||\pi||))!) \tag{23}$$

[7] For a positive integer n, $\nu_2(n)$ denotes the 2–adic norm of n, i.e., the exponent of 2 in the prime decomposition of n.

with equality occurring if and only if $|\pi| \leq ||\pi|| + 1$.

Proof. We may assume that $||\pi|| > 0$, i.e., that π is a non–empty partition. Write $|\pi| = ||\pi|| + m$ with some integer $m \geq 0$. By the inequality relating arithmetic and geometric mean, we have

$$2^{\nu_2(\prod_{j=1}^{\infty} j^{\pi_j})} \;\leq\; \prod_{j=1}^{\infty} j^{\pi_j} \;\leq\; \Big(1 + \frac{m}{||\pi||}\Big)^{||\pi||}.$$

On the other hand,

$$\nu_2((2(|\pi| - ||\pi||))!) \;\geq\; m + \frac{m-1}{2} + \frac{m-3}{2} = \frac{7m-5}{4}.$$

Since the sequence $\{(1+\frac{m}{\ell})^\ell\}_{\ell=1}^{\infty}$ is increasing for each fixed $m \geq 0$ and converges to e^m, validity of the inequality $\mathrm{e}^{4m} < 2^{7m-5}$ for some m implies (23) with strict inequality for all partitions π such that $|\pi| - ||\pi|| = m$ with this particular m. The latter inequality holds for all

$$m \;>\; \frac{5\log(2)}{7\log(2) - 4} \;\approx\; 4.0676207,$$

and a check of the remaining cases where $|\pi| - ||\pi|| \leq 4$ completes the proof. □

We can now proceed with our analysis of the function $\chi_q^*(\lambda)$. In Proposition 1 put $\mathfrak{G} = \mathfrak{H}(q)$, and write $\mathcal{B}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu)$ for $\mathcal{B}_\mu^{(\mathfrak{H}(q))}(\lambda_1, \ldots, \lambda_\mu)$. Multiply both sides of (15) by a sufficiently large odd number B depending only on q to obtain

$$B\, b_q(\lambda + 1) = \sum_{\mu=1}^{\mu_q} 2^{-(\nu_2(\mu!) + \mu\nu_2(m_q))} \sum_{\substack{\lambda_1, \ldots, \lambda_\mu > 0\\ \lambda_1 + \cdots + \lambda_\mu = \lambda}} \tilde{\mathcal{B}}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu) \prod_{j=1}^{\mu} b_q(\lambda_j), \quad \lambda \geq 1, \quad (24)$$

with integers $\tilde{\mathcal{B}}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu)$ satisfying

$$\nu_2(\tilde{\mathcal{B}}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu)) \;=\; \nu_2(\mathcal{B}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu)).$$

Decompose $\mathcal{B}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu)$ as

$$\mathcal{B}_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu) = \mu!\, A_\mu^{(q)} + \Theta_\mu^{(q)}(\lambda) + R_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu),$$

where

$$\Theta_\mu^{(q)}(\lambda) := \begin{cases} (\mu+1)!\,(\lambda - \mu)\, A_{\mu+1}^{(q)}/2, & \mu < \mu_q \\ 0, & \mu = \mu_q \end{cases}$$

and

$$R_\mu^{(q)}(\lambda_1, \ldots, \lambda_\mu) := \sum_{\nu=\mu+2}^{\mu_q} \sum_{\substack{\nu_1, \ldots, \nu_\mu \geq 0\\ \nu_1 + \cdots + \nu_\mu = \nu - \mu}} A_\nu^{(q)} \frac{\nu!}{(\nu_1 + 1) \ldots (\nu_\mu + 1)} \binom{\lambda_1 - 1}{\nu_1} \cdots \binom{\lambda_\mu - 1}{\nu_\mu}.$$

By Lemmas 1 and 2 we have for $\nu \geq \mu \geq 1$

$$\nu_2\Big(\frac{\nu!\,A_\nu^{(q)}}{(\nu_1+1)\dots(\nu_\mu+1)}\Big) \;\geq\; \nu_2(\nu!) \,+\, \nu\,\nu_2(m_q) \,-\, \nu_2((2(\nu-\mu))!)$$

with equality occurring at most in the cases when $\nu-\mu \leq 1$. It follows that for $\nu \geq \mu+2$

$$\begin{aligned}\nu_2\Big(\frac{2^{-(\nu_2(\mu!)+\mu\nu_2(m_q))}\,\nu!\,A_\nu^{(q)}}{(\nu_1+1)\dots(\nu_\mu+1)}\Big) &> \nu\,\nu_2(m_q)+\nu_2(\nu!)-\nu_2((2(\nu-\mu))!)-\nu_2(\mu!)-\mu\,\nu_2(m_q)\\ &\geq \nu \,-\, \mu \,+\, \nu_2(\nu!) \,-\, \nu_2(\mu!) \,-\, \nu_2((2(\nu-\mu))!)\\ &= \nu_2\Big(\binom{2\nu}{2\mu}\Big) \;\geq\; 0.\end{aligned}$$

Hence, for each $\mu \in [\mu_q]$, the term $R_\mu^{(q)}(\lambda_1,\dots,\lambda_\mu)$ is divisible by $2^{\nu_2(\mu!)+\mu\nu_2(m_q)}$, and

$$R_\mu^{(q)}(\lambda_1,\dots,\lambda_\mu)/2^{\nu_2(\mu!)+\mu\nu_2(m_q)}$$

is even. Furthermore, we claim that $\Theta_\mu^{(q)}(\lambda)$ is also divisible by $2^{\nu_2(\mu!)+\mu\nu_2(m_q)}$ for all $\mu \in [\mu_q]$, and that

$$\Theta_\mu^{(q)}(\lambda)/2^{\nu_2(\mu!)+\mu\nu_2(m_q)} \equiv \begin{cases}\binom{q/2}{\mu+1}\,\lambda, & \mu\equiv 0\,(2)\text{ and }\nu_2(q)=1\\ 0, & \text{otherwise}\end{cases} \quad \bmod 2. \tag{25}$$

This is certainly true if $\mu=\mu_q$. Hence, we may suppose that $\mu<\mu_q$ and consider divisibility of $(\mu+1)!\,A_{\mu+1}^{(q)}$ by $2^{1+\nu_2(\mu!)+\mu\nu_2(m_q)}$. Now, if μ is odd, then $\nu_2((\mu+1)!) > \nu_2(\mu!)$, and our claim follows from the fact that, by Lemma 1, $2^{(\mu+1)\nu_2(m_q)}$ divides $A_{\mu+1}^{(q)}$. If, on the other hand, μ is even, then $\nu_2((\mu+1)!)=\nu_2(\mu!)$, and Lemma 1 tells us that $(\mu+1)!\,A_{\mu+1}^{(q)}$ is divisible by $2^{1+\nu_2(\mu!)+\mu\nu_2(m_q)}$, and that

$$(\mu+1)!\,A_{\mu+1}^{(q)}/2^{1+\nu_2(\mu!)+\mu\nu_2(m_q)} \equiv 2^{\nu_2(m_q)-1}\binom{\mu_q}{\mu+1} \quad \bmod 2. \tag{26}$$

For $\nu_2(q)>1$ the right–hand side of (26) vanishes modulo 2. Similarly, if q is odd, then $\mu_q=q-1$ is even, and $\binom{\mu_q}{\mu+1}\equiv 0\,(2)$. However, if $\nu_2(q)=1$, then $m_q=q$, and $\mu_q=q/2$ is odd. Thus, our claim (25) is proved. Finally, again by Lemma 1, $2^{\nu_2(\mu!)+\mu\nu_2(m_q)}$ divides $\mu!\,A_\mu^{(q)}$ for every $\mu\in[\mu_q]$, and

$$\mu!\,A_\mu^{(q)}/2^{\nu_2(\mu!)+\mu\nu_2(m_q)} \equiv \binom{\mu_q}{\mu} \quad \bmod 2.$$

We conclude that $\tilde{\mathcal{B}}_\mu^{(q)}(\lambda_1,\dots,\lambda_\mu)$ is divisible by $2^{\nu_2(\mu!)+\mu\nu_2(m_q)}$ and that

$$\tilde{\mathcal{B}}_\mu^{(q)}(\lambda_1,\dots,\lambda_\mu)/2^{\nu_2(\mu!)+\mu\nu_2(m_q)} \equiv \begin{cases}0, & \nu_2(q)=1\,\&\,\mu\equiv 0\,(2)\,\&\,\lambda\equiv 1\,(2)\\ \binom{\mu_q}{\mu}, & \text{otherwise}\end{cases} \quad \bmod 2. \tag{27}$$

Evaluating (24) modulo 2 in the light of (27) we find for the function $\chi_q^*(\lambda)$ the $GF(2)$–recurrence relation

$$\chi_q^*(\lambda+1) = \sum_{\mu=1}^{\mu_q} \sum_{\substack{\lambda_1,\ldots,\lambda_\mu>0\\ \lambda_1+\cdots+\lambda_\mu=\lambda}} \Big[1+(1+\mu)\,\lambda\,\delta_{1,\nu_2(q)}\Big] \binom{\mu_q}{\mu} \chi_q^*(\lambda_1)\ldots\chi_q^*(\lambda_\mu)$$
$$(\lambda\geq 1,\ \chi_q^*(1)=1). \tag{28}$$

Introduce the generating series

$$X_q^*(z) := 1 \,+ \sum_{\lambda=1}^{\infty} \chi_q^*(\lambda)\,z^\lambda \,\in\, GF(2)[[z]].$$

Multiplying both sides of (28) by z^λ and summing over $\lambda \geq 1$, the left–hand side becomes

$$\sum_{\lambda=1}^{\infty} \chi_q^*(\lambda+1)\,z^\lambda = z^{-1}\Big[1+z+X_q^*(z)\Big],$$

while the corresponding right–hand side is the sum of

$$\Sigma_1 := \sum_{\lambda=1}^{\infty}\sum_{\mu=1}^{\mu_q} \sum_{\substack{\lambda_1,\ldots,\lambda_\mu>0\\ \lambda_1+\cdots+\lambda_\mu=\lambda}} \binom{\mu_q}{\mu} \chi_q^*(\lambda_1)\ldots\chi_q^*(\lambda_\mu)\,z^\lambda$$

and

$$\Sigma_2 := \sum_{\lambda=1}^{\infty}\sum_{\mu=1}^{\mu_q} \sum_{\substack{\lambda_1,\ldots,\lambda_\mu>0\\ \lambda_1+\cdots+\lambda_\mu=\lambda}} (1+\mu)\,\lambda\,\delta_{1,\nu_2(q)} \binom{\mu_q}{\mu} \chi_q^*(\lambda_1)\ldots\chi_q^*(\lambda_\mu)\,z^\lambda.$$

By the binomial law in the ring $GF(2)[[z]]$

$$\Sigma_1 = \sum_{\mu=1}^{\mu_q} \binom{\mu_q}{\mu} \Big(1+X_q^*(z)\Big)^\mu = 1+\big(X_q^*(z)\big)^{\mu_q}.$$

Also,

$$\Sigma_2 = \delta_{1,\nu_2(q)}\,z \sum_{\mu=1}^{\mu_q} (1+\mu)\binom{\mu_q}{\mu}\left[\Big(1+X_q^*(z)\Big)^\mu\right]' = 0.$$

Summarizing the preceding discussion we have the following result.

Proposition 2. *For every integer $q \geq 3$ the generating function $X_q^*(z)$ satisfies the identity*

$$X_q^*(z) = 1 + z\big(X_q^*(z)\big)^{\mu_q}. \tag{29}$$

Equivalently, for every $q \geq 3$ the characteristic function $\chi_q^*(\lambda)$ satisfies the $GF(2)$–recursion

$$\chi_q^*(\lambda+1) = \sum_{\substack{\pi \vdash \lambda \\ ||\pi|| \leq \mu_q}} \binom{\mu_q}{||\pi||} \frac{||\pi||!}{\prod_{j=1}^{\infty} \pi_j!} \prod_{j=1}^{\infty} \left(\chi_q^*(j)\right)^{\pi_j}, \quad \lambda \geq 1 \tag{30}$$

starting from $\chi_q^*(1) = 1$.

Identity (29) can be interpreted as providing a recursive reconstruction of the set Π_q^*. Define $\Pi_q^*(\lambda) := \Pi_q^* \cap [\lambda]$. Rewriting (29) in the form

$$\sum_{\lambda \in \Pi_q^*} z^\lambda \;=\; z \left[1 \;+\; \sum_{\lambda \in \Pi_q^*} z^\lambda\right]^{\mu_q}$$

and comparing coefficients we find that $\Pi_q^*(1) = \{1\}$, and, assuming $\Pi_q^*(\lambda)$ to be known for some $\lambda \geq 1$, we see that $\Pi_q^*(\lambda+1)$ is determined by the condition that $\lambda + 1 \in \Pi_q^*$ if and only if the number of representations of λ in the form $\lambda = \lambda_1 + \cdots + \lambda_{\mu_q}$ with $\lambda_j \in \Pi_q^*(\lambda) \cup \{0\}$ is odd.

4. The free parity pattern of a Hecke group

4.1. **The results.** In this section we will exploit the identity (29) to obtain results concerning the parity patterns Π_q^*. Equation (30) tells us in particular that Π_q^* is already determined by the free rank μ_q, and the question arises whether, conversely, the parity pattern Π_q^* also determines μ_q, or whether there exist Hecke groups having different free ranks while exhibiting the same free parity pattern. Our first result shows that the latter situation cannot arise.

Theorem 1. *Let $q_1, q_2 \geq 3$ be integers. Then we have $\Pi_{q_1}^* = \Pi_{q_2}^*$ if and only if $\mu_{q_1} = \mu_{q_2}$.*

Proof. We observed already that $\mu_{q_1} = \mu_{q_2}$ implies $\Pi_{q_1}^* = \Pi_{q_2}^*$. Conversely, let $q_1, q_2 \geq 3$ be integers with $\Pi_{q_1}^* = \Pi_{q_2}^* =: \Pi^*$. Then $X_{q_1}^*(z) = X_{q_2}^*(z) =: X^*(z)$, and (29) implies that $(X^*(z))^{\mu_{q_1}} = (X^*(z))^{\mu_{q_2}}$. Suppose without loss of generality that $\mu_{q_1} \leq \mu_{q_2}$, and rewrite the last equation as

$$(X^*(z))^{\mu_{q_1}} \left[(X^*(z)^{\vartheta} - 1\right] = 0, \tag{31}$$

where $\vartheta := \mu_{q_1} - \mu_{q_2} \geq 0$. Since $X^*(z) \neq 0$ and $GF(2)[[z]]$ has no zero divisors, we find using the binomial law in $GF(2)[[z]]$ the $GF(2)$–relation

$$1 = (X^*(z))^{\vartheta} = \sum_{\nu=0}^{\vartheta} \binom{\vartheta}{\nu} \Bigg(\sum_{\lambda \in \Pi^*} z^\lambda\Bigg)^{\nu}. \tag{32}$$

Using the fact that $\chi_q^*(1) = 1$ for every $q \geq 3$ and comparing coefficients we deduce that $\binom{\vartheta}{\nu} \equiv 0\,(2)$ for all $\nu \in [\vartheta]$, which is impossible for $\vartheta > 0$. Hence, we must have $\vartheta = 0$. $\square$

Next, we prove that the parity patterns Π_q^* are always infinite, and that certain infinite sets of positive integers cannot occur as free parity pattern of a Hecke group. For an integer $q \geq 3$ define $\alpha_q^* := \min_{\lambda \in \Pi_q^* \setminus \{1\}} \lambda$.

Theorem 2. (i) *For every integer $q \geq 3$ the set Π_q^* is infinite.*
(ii) *The sets $\mathcal{C}_m = 1 + m\mathbb{N}_0$ with $m \in \mathbb{N}$ do not occur as free parity pattern of a Hecke group.*
(iii) *Let $\alpha^* \geq 2$ be an integer. Then there exists an integer $q \geq 3$ with $\alpha^* = \alpha_q^*$ (i.e. the set $\{1, \alpha^*\}$ can be extended to a free parity pattern of some Hecke group) if and only if $\alpha^* - 1$ is a 2–power.*

Proof. (i) Suppose that for some $q \geq 3$ the set Π_q^* is finite. Then $X_q^*(z)$ is a polynomial over $GF(2)$ of degree $d := deg(X_q^*(z)) > 0$. Comparing the degrees on both sides of (29) we find that $d = d\mu_q + 1$, which is impossible.

(ii) Suppose that $\Pi_q^* = 1 + m\mathbb{N}_0$ for some $m \geq 1$ and $q \geq 3$. Then

$$X_q^*(z) = \frac{1 + z + z^m}{1 + z^m},$$

and (29) implies

$$(1 + z^m)^{\mu_q - 1} = (1 + z + z^m)^{\mu_q}.$$

Comparing degrees shows that the latter equation is impossible.

(iii) Suppose that we have $\{1, \alpha^*, \dots\} = \Pi_q^*$ for some $\alpha^* \geq 2$ and some $q \geq 3$. Then

$$X_q^*(z) = 1 \,+\, z \,+\, z^{\alpha^*} \,+\, \text{higher powers of } z.$$

Inserting this equation into (29) and comparing coefficients we find that

$$\binom{\mu_q}{1}, \dots, \binom{\mu_q}{\alpha^* - 2} \equiv 0 \ (2) \quad \text{and} \quad \binom{\mu_q}{\alpha^* - 1} \equiv 1 \ (2),$$

i.e., the μ_q–th row of Pascal's triangle viewed modulo 2 starts with a string of the form

$$1 \ \underbrace{0 \dots 0}_{\alpha^* - 2} \ 1, \quad \alpha^* \geq 2. \tag{33}$$

Conversely, if Pascal's triangle contains a row which, when evaluated modulo 2, starts with a section of the form (33) for some $\alpha^* \geq 2$, then choosing $q \geq 3$ such that μ_q equals the number of this row (which we can without loss of generality assume to be greater than 1) we find that $\alpha_q^* = \alpha^*$. Hence, given any integer $\alpha^* \geq 2$, the set $\{1, \alpha^*\}$ extends to a free parity pattern of some Hecke group if and only if Pascal's triangle contains a row which starts with a string of the form (33) when considered modulo 2. However, if p is a prime and $a = \sum_{i=0}^{\infty} a_i^{(p)} p^i$ and $b = \sum_{i=0}^{\infty} b_i^{(p)} p^i$ are positive integers written in base p, then it is well known[8] that

$$\binom{a}{b} \equiv \prod_{i=0}^{\infty} \binom{a_i^{(p)}}{b_i^{(p)}} \quad \bmod p; \tag{34}$$

[8] Cf. for instance [2, Theorem 3.4.1].

in particular, $\binom{a}{b} \equiv 1\ (2)$ if and only if $a_i^{(2)} \geq b_i^{(2)}$ for all $i \geq 0$. From this observation it follows easily that a row starting with a string of the form (33) exists in Pascal's triangle modulo 2 if and only if α^* is of the form $\alpha^* = 2^r + 1$ with some $r \geq 0$, whence the claim. □

Call a sequence $\underline{\alpha} = \{\alpha_i\}_0^\infty \in \mathbb{N}_0^{\mathbb{N}_0}$ *finitary* if there exists some $\mu \in \mathbb{N}_0$ such that $\alpha_i = 0$ for all $i > \mu$. The smallest such μ is called the *length* $\ell(\underline{\alpha})$. The *norm* $||\underline{\alpha}||$ of a finitary sequence $\underline{\alpha}$ is defined as $||\underline{\alpha}|| = \sum_{i=0}^\infty \alpha_i$. Let

$$\mathcal{A} := \Big\{ \underline{\alpha} \in \mathbb{N}_0^{\mathbb{N}_0} :\ \underline{\alpha} \text{ is finitary and } \alpha_0 = 1 \Big\}.$$

Our next result gives a fairly explicit description of the parity patterns Π_q^*.

Theorem 3. *For every $q \geq 3$,*

$$\Pi_q^* = \left\{ \lambda \in \mathbb{N} :\ \sum_{\substack{\underline{\alpha} \in \mathcal{A} \\ ||\underline{\alpha}|| = \lambda}} \prod_{i=0}^\infty \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} \equiv 1 \bmod 2 \right\}.$$

Proof. Using the identity (29) plus the binomial law in $GF(2)[[z]]$, a straightforward induction shows that for every $\mu \in \mathbb{N}_0$ we have the $GF(2)$–relation

$$X_q^*(z) = 1\ +\ \sum_{\substack{\underline{\alpha} \in \mathcal{A} \\ \ell(\underline{\alpha}) \leq \mu}} \prod_{i=0}^\infty \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} z^{||\underline{\alpha}||}\ +\ \mathcal{R}_\mu(z),$$

where

$$\mathcal{R}_\mu(z) := \sum_{\alpha_1, \dots, \alpha_{\mu+1} > 0} \binom{\mu_q}{\alpha_1} \prod_{i=1}^{\mu} \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} z^{1+\alpha_1+\cdots+\alpha_{\mu+1}} \left(X_q^*(z)\right)^{\alpha_{\mu+1}\, \mu_q}.$$

By the ultrametric inequality for the norm on the algebra of formal power series over a ring with identity element[9] this implies that for every $\mu \in \mathbb{N}_0$,

$$\begin{aligned} \left|\left| X_q^*(z) - \left[1 + \sum_{\underline{\alpha} \in \mathcal{A}} \prod_{i=0}^\infty \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} z^{||\underline{\alpha}||} \right] \right|\right| \ &\leq\ \max\left\{ ||\mathcal{R}_\mu(z)||, \left|\left| \sum_{\substack{\underline{\alpha} \in \mathcal{A} \\ \ell(\underline{\alpha}) > \mu}} \prod_{i=0}^\infty \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} z^{||\underline{\alpha}||} \right|\right| \right\} \\ &\leq\ 2^{-(\mu+2)}. \end{aligned}$$

Thus, letting $\mu \to \infty$ yields the $GF(2)$–relation

$$X_q^*(z)\ =\ 1 + \sum_{\underline{\alpha} \in \mathcal{A}} \prod_{i=0}^\infty \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} z^{||\underline{\alpha}||}\ =\ 1 + \sum_{\lambda=1}^\infty \left(\sum_{\substack{\underline{\alpha} \in \mathcal{A} \\ ||\underline{\alpha}|| = \lambda}} \prod_{i=0}^\infty \binom{\alpha_i\, \mu_q}{\alpha_{i+1}} \right) z^\lambda.$$

Theorem 3 follows now by comparing coefficients. □

[9] See [12, Chap. 3] or [35, Chap. VII, §1] for the definition and properties of this norm.

As is apparent from Theorem 3, the parity patterns Π_q^* will in general not lend themselves to a "nice" and straightforward characterization, but rather tend to exhibit a peculiar type of fractal behaviour. The only exception occurs when μ_q is a 2–power. Thus, while a canonical generalization of the free parity pattern met in the modular group $\mathfrak{H}(3)$ and in $\mathfrak{H}(4)$ to all Hecke groups does not exist, this type of pattern characterizes two infinite series of Hecke groups. For an integer $q \geq 3$ define

$$\Lambda_q^* := \left\{ \frac{\mu_q^\sigma - 1}{\mu_q - 1} : \ \sigma = 1, 2, \dots \right\},$$

i.e., Λ_q^* is the set of partial sums of the geometric series $\sum_{\sigma=0}^\infty \mu_q^\sigma$ generated by the free rank μ_q of $\mathfrak{H}(q)$.

Theorem 4. *Let $q \geq 3$ be an integer. Then the following assertions are equivalent:*

(i) $\Pi_q^* = \Lambda_q^*$.

(ii) $\chi_q^*(\lambda) = 0$ *for* $2 \leq \lambda \leq \mu_q$.

(iii) q *or* $q-1$ *is a 2–power.*

Our proof of Theorem 4 is based on Theorem 3, equation (30), and the fact, following from (34), that we have $\binom{n}{k} \equiv 0\,(2)$ for some $n \geq 1$ and all $0 < k < n$ if and only if n is a 2–power.

Proof of Theorem 4. Since (i) clearly implies (ii), it suffices to prove the implications (ii)⇒(iii) and (iii)⇒(i). Assume first that neither q nor $q-1$ is a 2–power. Then μ_q is not a 2–power, and the set

$$\mathcal{M} = \left\{ \mu \in [\mu_q - 1] : \ \binom{\mu_q}{\mu} \equiv 1\,(2) \right\}$$

is non–empty. Let $\mu_0 := \min_{\mu \in \mathcal{M}} \mu$. Then $2 \leq \mu_0 + 1 \leq \mu_q$, and (30) gives $\chi_q^*(\mu_0 + 1) = \chi_q^*(1) = 1$, contradicting (ii). This proves the implication (ii)⇒(iii).[10] Now suppose that q or $q-1$ (and hence also μ_q) is a 2–power. Then, given a finitary sequence $\underline{\alpha} \in \mathcal{A}$, we will have $\prod_{i=0}^\infty \binom{\alpha_i\,\mu_q}{\alpha_{i+1}} \equiv 1\,(2)$ if and only if $\underline{\alpha}$ is of the form $\underline{\alpha} = (1, \mu_q, \mu_q^2, \dots, \mu_q^\sigma, 0, \dots)$ for some $\sigma \geq 0$. If $\lambda \in \Pi_q^*$, then by Theorem 3 there exists $\underline{\alpha} \in \mathcal{A}$ such that $||\underline{\alpha}|| = \lambda$ and $\prod_{i=0}^\infty \binom{\alpha_i\,\mu_q}{\alpha_{i+1}} \equiv 1\,(2)$, hence by the above observation we must have $\lambda \in \Lambda_q^*$. Conversely, if $\lambda \in \Lambda_q^*$, then, since λ has a unique expansion in base μ_q, there exists precisely one finitary sequence $\underline{\alpha} \in \mathcal{A}$ with $||\underline{\alpha}|| = \lambda$ and $\prod_{i=0}^\infty \binom{\alpha_i\,\mu_q}{\alpha_{i+1}} \equiv 1\,(2)$, and Theorem 3 implies that $\lambda \in \Pi_q^*$. Hence, $\Pi_q^* = \Lambda_q^*$, and the theorem is proved. □

By specializing Theorem 4 to the case when q is a prime number, we obtain a characterization of Fermat primes among the set of all odd primes.

Corollary 1. *Let $q > 2$ be a prime. Then the following assertions are equivalent:*

(i) $\Pi_q^* = \Lambda_q^* = \left\{ \dfrac{(q-1)^\sigma - 1}{q-2} : \ \sigma = 1, 2, \dots \right\}$.

[10] Given that neither q nor $q-1$ is a 2–power, the number $\mu_0 + 1$ constructed in the proof of the implication (ii)⇒(iii) is in fact the smallest integer for which the patterns Π_q^* and Λ_q^* differ as to their containing or not containing this number, i.e., we have $\min_{\lambda \in \Pi_q^* \,\Delta\, \Lambda_q^*} \lambda = \mu_0 + 1$.

(ii) $\chi_q^*(\lambda) = 0$ *for* $2 \leq \lambda \leq q-1$.

(iii) q *is a Fermat prime.*

4.2. **An example.** Here we consider the groups $\mathfrak{H}(q)$ with $q = 2(2^\rho+1)$ and $\rho \geq 1$. These are the Hecke groups for which $\mu_q - 1$ is a 2–power. For a positive integer n and a prime p denote by $\lfloor n \rfloor^{(p)}$ the largest p–power which is less or equal to n. We will make use of the following observation, which is a straightforward consequence of (34).

Lemma 3. *Let* $n, \lambda \geq 1$ *be integers, let* p *be a prime, and suppose that the multinomial coefficient* $\binom{n}{n_1,\dots,n_\lambda}$ *is not divisible by* p. *Then there exists some* $j \in [\lambda]$ *such that* $n_j \geq \lfloor n \rfloor^{(p)}$.

Analysing equation (30) by means of Lemma 3, we find that for such q the characteristic function $\chi_q^*(\lambda)$ satisfies the recurrence relation

$$\chi_q^*(\lambda+1) \;=\; \chi_q^*(\lambda) \;+ \sum_{1 \leq \mu < \lambda/2^\rho} \chi_q^*(\mu)\,\chi_q^*(\lambda - 2^\rho \mu) \;+\; \begin{cases} \chi_q^*(\lambda/2^\rho), & 2^\rho \mid \lambda \\ 0, & 2^\rho \nmid \lambda \end{cases}$$
$$(\lambda \geq 1,\ \chi_q^*(1) = 1).$$

Defining $\chi_q^*(0) := 1$ this recursion can be rewritten as

$$\chi_q^*(\lambda+1) \;=\; \sum_{0 \leq \mu \leq \lambda/2^\rho} \chi_q^*(\mu)\,\chi_q^*(\lambda - 2^\rho\mu), \quad \lambda \geq 0, \tag{35}$$

starting from $\chi_q^*(0) = 1$, which is equivalent to the relation

$$X_q^*(z) = \frac{1}{1 + zX_q^*(z^{2^\rho})}. \tag{36}$$

Putting $2^\rho =: \beta$ and iterating (36) we find for the generating function $X_q^*(z)$ the expansion

$$X_q^*(z) = \cfrac{1}{1 + \cfrac{z}{1 + \cfrac{z^\beta}{1 + \cfrac{z^{\beta^2}}{1 + \ddots}}}} \tag{37}$$

as a continued fraction over $GF(2)$. The approximands of numerator and denominator are given recursively as

$$A_{\nu+1}(z) = A_\nu(z) + z^{\beta^{\nu-1}} A_{\nu-1}(z) \quad (\nu \geq 1;\ A_0 = 0,\ A_1 = 1) \tag{38}$$

respectively

$$B_{\nu+1}(z) = B_\nu(z) + z^{\beta^{\nu-1}} B_{\nu-1}(z) \quad (\nu \geq 1;\ B_0 = B_1 = 1). \tag{39}$$

From these recursions one immediately infers by induction that for $\nu \geq 1$

$$\operatorname{supp}\big(A_\nu(z)\big) \subseteq \Big[0, \sum_{1 \leq i < \nu/2} \beta^{\nu-2i}\Big] \;\text{ and }\; \operatorname{supp}\big(B_\nu(z)\big) \subseteq \Big[0, \sum_{1 \leq i \leq \nu/2} \beta^{\nu-2i}\Big],$$

where, in both cases, the endpoints of the right–hand interval are contained in the corresponding support. From this observation and the recursions (38) and (39) it follows that for each $\nu \geq 2$ the polynomial $A_{\nu+1}(z)$ extends $A_\nu(z)$, and that the smallest power of z newly introduced when passing from $A_\nu(z)$ to $A_{\nu+1}(z)$ is $z^{\beta^{\nu-1}}$. Similarly, $B_{\nu+1}(z)$ extends $B_\nu(z)$ for every $\nu \geq 2$, and, again, the smallest power of z newly introduced when passing from $B_\nu(z)$ to $B_{\nu+1}(z)$ is $z^{\beta^{\nu-1}}$. In particular, we observe that the limits $A(z) = \lim_{\nu\to\infty} A_\nu(z)$ and $B(z) = \lim_{\nu\to\infty} B_\nu(z)$ exist in $GF(2)[[z]]$, and the identity (37) exhibits the generating function $X_q^*(z)$ as the quotient $X_q^*(z) = A(z)/B(z)$ of these two formal power series. Introducing the generating functions

$$F(x,z) := \sum_{\nu=0}^{\infty} A_\nu(z)\, x^{\beta^\nu} \quad \text{and} \quad G(x,z) := \sum_{\nu=0}^{\infty} B_\nu(z)\, x^{\beta^\nu}$$

the recursions (38) and (39) are found to be equivalent to the functional equations

$$F(x,z) + F(x^\beta, z) + F(x^{\beta^2} z, z) + x^\beta = 0 \tag{40}$$

respectively

$$G(x,z) + G(x^\beta, z) + G(x^{\beta^2} z, z) + x = 0 \tag{41}$$

for $F(x,z)$ and $G(x,z)$. The reader may find it instructive to try to use (40) and (41) to obtain an explicit formula for the power series $F(x,z)$ and $G(x,z)$, and hence for the series $A(z)$ and $B(z)$.

5. The parity patterns of the groups $\widetilde{\mathfrak{H}}(q)$

For an integer $q \geq 3$ let $\widetilde{\mathfrak{H}}(q) := C_q * C_q$, and denote by $\tilde{\chi}_q(n)$ the number $s_n(\widetilde{\mathfrak{H}}(q))$ of index n subgroups in $\widetilde{\mathfrak{H}}(q)$ considered modulo 2, so that $\tilde{\chi}_q$ is simply the characteristic function of the set $\widetilde{\Pi}_q := \Pi(\widetilde{\mathfrak{H}}(q)) \subseteq \mathbb{N}$. The purpose of this section is to establish a recursive description of the function $\tilde{\chi}_q(n)$, derived from a differential equation for the generating function $\widetilde{X}_q(z) := \sum_{n=0}^{\infty} \tilde{\chi}_q(n+1)\, z^n$, and to exploit this recursion (respectively the differential equation equivalent to it) to investigate the parity patterns $\widetilde{\Pi}_q$. The results of this section depend upon certain properties of the infinite rectangular array

$$\Big(|\operatorname{Hom}(C_q, S_\mu)| \cdot |\operatorname{Hom}(C_q, S_\nu)|\Big)_{\mu,\nu \geq 0},$$

which will be established in the next section.

5.1. **A recursive description of the function $\tilde{\chi}_q(n)$.** Put $h_n(q) := |\operatorname{Hom}(C_q, S_n)|$ with the convention that $h_0(q) = 1$ and $h_n(q) = 0$ for $n < 0$. Our starting point is the recurrence relation[11]

$$h_n(q) = \sum_{d|q} (n-1)_{d-1}\, h_{n-d}(q), \quad (n \geq 1,\ h_0(q) = 1), \tag{42}$$

which follows from the identity

$$\sum_{n=0}^{\infty} h_n(q) z^n/n! = \exp\left(\sum_{d|q} z^d/d\right) \tag{43}$$

due to Chowla, Herstein, and Scott [3] by differentiating and comparing coefficients.[12] Squaring (42), multiplying both sides by $z^{n-1}/(n-1)!$, and summing over $n \geq 1$ gives

$$\begin{aligned}\sum_{n=1}^{\infty} h_n^2(q)\, z^{n-1}/\,(n-1)! &= \sum_{n=1}^{\infty}\sum_{d|q} (n-1)_{d-1}^2\, h_{n-d}^2(q)\, z^{n-1}/\,(n-1)!\\ &+\ 2\sum_{n=1}^{\infty} \sum_{\substack{d_1,d_2|q\\ d_1<d_2}} (n-1)_{d_1-1}\,(n-1)_{d_2-1}\, h_{n-d_1}(q)\, h_{n-d_2}(q)\, z^{n-1}/\,(n-1)!.\end{aligned}$$

Interchanging the summations over n and q respectively n and the pairs (d_1, d_2), introducing the series

$$\widetilde{H}_q(z) = \sum_{n=0}^{\infty} h_n^2(q)\, z^n/\,n! = \sum_{n=0}^{\infty} |\operatorname{Hom}(\widetilde{\mathfrak{H}}(q), S_n)|\, z^n/\,n!,$$

and rewriting the individual terms occurring in the last equation, we obtain the relation

$$\widetilde{H}_q'(z) = \sum_{d|q} z^{d-1}\big(z^{d-1}\widetilde{H}_q(z)\big)^{(d-1)} + 2\sum_{\substack{d_1,d_2|q\\ d_1<d_2}} z^{d_1-1}\left(z^{d_2-1}\sum_{n=0}^{\infty} h_n(q)h_{n+d_2-d_1}(q)z^n/n!\right)^{(d_1-1)}.$$

Applying Leibniz's formula for the higher derivatives of a product function to the latter equation, dividing both sides of the resulting identity by $\widetilde{H}_q(z)$, and using the fact that, by Dey's formula [4, Theorem 6.10],

$$\widetilde{S}_q(z) := \sum_{n=0}^{\infty} s_{n+1}(\widetilde{\mathfrak{H}}(q))\, z^n = \widetilde{H}_q'(z)/\widetilde{H}_q(z), \tag{44}$$

[11]For a ring R with identity element 1, an element $r \in R$, and an integer k, we set $(r)_k := \prod_{\nu=0}^{k-1}(r-\nu)$, with the usual convention that an empty product should equal 1. This is the falling factorial r of order k. Its analogue $\langle r\rangle_k = \prod_{\nu=0}^{k-1}(r+\nu)$, the rising factorial r of order k, is sometimes called a Pochhammer symbol.

[12]More general results concerning the enumeration of permutation representations respectively wreath product representations of (arbitrary) groups, which contain formulae (11), (43), and (44) below as special cases, can be found in [6] and [26].

we find that

$$\begin{aligned}\widetilde{S}_q(z) = \sum_{d\mid q}\sum_{\nu=0}^{d-1}\binom{d-1}{\nu}(d-1)_{d-\nu-1}\,z^{d+\nu-1}\,\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z)\\ +\,2\sum_{\substack{d_1,d_2\mid q\\ d_1<d_2}}\sum_{\nu=0}^{d_1-1}\binom{d_1-1}{\nu}(d_2-1)_{d_1-\nu-1}\,z^{d_2+\nu-1}\,\mathcal{R}_q^{d_2-d_1,\nu}(z),\end{aligned}\tag{45}$$

where, for $q \geq 3$, $\mu > 0$, and $\nu \geq 0$

$$\mathcal{R}_q^{\mu,\nu}(z) := \left(\sum_{n=0}^{\infty} h_n(q)\,h_{n+\mu}(q)\,z^n/n!\right)^{(\nu)} \Big/\, \widetilde{H}_q(z).$$

We now make use of the facts, to be proved among other things in the next section, that the series $\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z)$ is an integral power series for every $\nu \geq 0$, and that

$$\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z) \equiv \sum_{\mu=0}^{\lfloor \nu/2\rfloor}\binom{\nu}{2\mu}\big(\widetilde{S}_q'(z)\big)^{\mu}\big(\widetilde{S}_q(z)\big)^{\nu-2\mu} \bmod 2,\quad \nu \geq 0. \tag{46}$$

Also, at this stage our main technical hypothesis comes into play, which is the following.

For every $q \geq 3$, each $0 < \mu < q$, and every $0 \leq \nu \leq q-2$ the series $\mathcal{R}_q^{\mu,\nu}(z)$, viewed as a power series, has integral coefficients. (47)

Again, this will be established in the next section. Taking into account (45), (46), and (47), we find for the series $\widetilde{X}_q(z)$ the differential equation

$$\widetilde{X}_q(z) = \sum_{d\mid q}\sum_{\mu\geq 0} z^{2d-3}\big(\widetilde{X}_q'(z)\big)^{\mu}\big(\widetilde{X}_q(z)\big)^{d-2(\mu+1)}\left[\binom{d-1}{2\mu}z\,\widetilde{X}_q(z) + (d-1)\binom{d-2}{2\mu}\right] \tag{48}$$

over $GF(2)$. Equation (48), which describes the dynamics of the parity pattern $\widetilde{\Pi}_q$, is the counterpart for the group $\widetilde{\mathfrak{H}}(q)$ and the arithmetic function $s_n(\widetilde{\mathfrak{H}}(q))$ of the algebraic identity (29) governing the series $X_q^*(z)$. Comparing coefficients in (48) one obtains a recurrence relation for the function $\tilde{\chi}_q(n)$, which we do not bother to write down explicitly, but whose existence serves to show that equation (48) uniquely determines its solution $\widetilde{X}_q(z)$. The first conclusion to be drawn from equation (48) is that for q odd we have $\widetilde{X}_q'(z) = 0$, i.e., the parity pattern $\widetilde{\Pi}_q$ consists only of odd numbers. Hence, for such q, the series $\widetilde{X}_q(z)$ satisfies the algebraic identity

$$\widetilde{X}_q(z) = 1 + \sum_{1<d\mid q} z^{2(d-1)}\big(\widetilde{X}_q(z)\big)^{d-1}, \tag{49}$$

and the corresponding recurrence relation for the characteristic function $\tilde{\chi}_q(n)$ is given by

$$\tilde{\chi}_q(n+1) = \sum_{1<d|q} \sum_{\substack{\pi\vdash n-2(d-1)\\ ||\pi||\leq d-1}} \binom{d-1}{||\pi||} \frac{||\pi||!}{\prod_{j=1}^{\infty}\pi_j!} \prod_{j=1}^{\infty} \big(\tilde{\chi}_q(j+1)\big)^{\pi_j}$$
$$(n\geq 1,\ \tilde{\chi}_q(1)=1,\ q \text{ odd}). \quad (50)$$

An immediate consequence of (50) is that for q odd we have

$$\tilde{\chi}_q(2) = \tilde{\chi}_q(3) = \cdots = \tilde{\chi}_q(2(p(q)-1)) = 0 \quad\text{and}\quad \tilde{\chi}_q(2p(q)-1) = 1,$$

where $p(q)$ denotes the smallest prime divisor of q.

5.2. **The parity patterns $\widetilde{\Pi}_q$.** Here we exploit the differential equation (48) to obtain results concerning the parity patterns of the groups $\mathfrak{H}(q)$. We begin by settling the case when q is even, after which we can dispose of (48) in favour of the simpler identity (49).

Theorem 5. *If $q>2$ is even, then $\widetilde{\Pi}_q = \mathbb{N}$.*

Proof. In (48) put $\widetilde{X}_q(z) = (1+z)^{-1}$. Upon multiplication with $(1+z)^{q-1}$ the resulting equation becomes

$$(1+z)^{q-2} = \sum_{(d,\mu)} z^{2d-3}(1+z)^{q-d}\big[dz+d-1\big], \quad (51)$$

where the right–hand sum extends over all pairs of non–negative integers (d,μ) such that $d \mid q$, $\mu\geq 0$, and $\binom{d-1}{2\mu}\equiv 1(2)$. As the terms of this sum are independent of μ, we can simplify (51) by determining for which divisors d of q the number of integers μ with $\mu\geq 0$ and $\binom{d-1}{2\mu}\equiv 1(2)$ is odd. Using (34) we find that if d is odd this happens exactly for $d=1$, whereas if d is even, we must have $d=2$. Thus, since q is even, equation (51) (and hence (48) with $\widetilde{X}_q(z)=(1+z)^{-1}$) is equivalent to the $GF(2)$–relation

$$(1+z)^{q-2} = (1+z)^{q-1} + z(1+z)^{q-2},$$

which obviously holds. Since the differential equation (48) has a unique solution, we conclude that for q even indeed $\widetilde{\Pi}_q=\mathbb{N}$ as claimed. □

As we have seen in Section 4, the free parity pattern Π_q^* determines the free rank μ_q of the associated Hecke group $\mathfrak{H}(q)$, and hence determines the structure of $\mathfrak{H}(q)$ up to finitely many (in fact at most two) isomorphism types. The corresponding statement for the parity patterns $\widetilde{\Pi}_q$ fails to hold in the light of Theorem 5. However, if we restrict attention to the case when q is odd, then the following analogue of Theorem 1 holds.

Theorem 6. *Let $q_1, q_2\geq 3$ be odd integers, and suppose that $\widetilde{\Pi}_{q_1} = \widetilde{\Pi}_{q_2}$. Then we have $q_1=q_2$.*

Proof. Put $\widetilde{X}_{q_1}(z) = \widetilde{X}_{q_2}(z) =: \widetilde{X}(z)$, and consider the equation

$$\sum_{d \in D(q_1) \Delta D(q_2)} z^{2(d-1)} \left(\widetilde{X}(z)\right)^{d-1} = 0, \tag{52}$$

which follows from (49). Here, $D(q)$ is the set of divisors of a positive integer q, and Δ denotes the symmetric difference of sets. For $q_1 \neq q_2$ the left–hand side Σ of (52) would be of order $\mathrm{ord}(\Sigma) = 2(d_1 - 1)$, where $d_1 := \min_{d \in D(q_1) \Delta D(q_2)} d$, in particular we would have $\Sigma \neq 0$. Hence, we must have $q_1 = q_2$. □

For an integer $q \geq 3$ define $\tilde{\alpha}_q := \min_{n \in \widetilde{\Pi}_q \setminus \{1\}} n$, and as before let $p(q)$ be the smallest prime divisor of q. Our next result summarizes some general properties of the parity patterns $\widetilde{\Pi}_q$ for q odd.

Theorem 7. *Let $q \geq 3$ be an odd integer. Then*

(i) *the set $\widetilde{\Pi}_q$ is infinite, and consists only of odd integers,*

(ii) *for every $m \in 2\mathbb{N}$ we have $\widetilde{\Pi}_q \neq 1 + m\mathbb{N}_0$,*

(iii) *we have $\tilde{\alpha}_q = 2p(q) - 1$.*

Proof. (i) We have already observed that for odd $q \geq 3$ the parity pattern $\widetilde{\Pi}_q$ consists only of odd numbers. Assume that for some such q the set $\widetilde{\Pi}_q$ is finite. Then $\widetilde{X}_q(z)$ is a non–vanishing polynomial over $GF(2)$, of degree d_q say. Comparing degrees on both sides of (49) we find that $d_q = (q-1)(d_q + 2)$, which is impossible.

(ii) Suppose that $\widetilde{\Pi}_q = 1 + m\mathbb{N}_0$ for some $m \in 2\mathbb{N}$. Then $\widetilde{X}_q(z) = (1 + z^m)^{-1}$, and (49) implies

$$(1 + z^m)^{q-2} = \sum_{d \mid q} z^{2(d-1)} (1 + z^m)^{q-d}.$$

Putting $z = 1$ in this equation yields $0 = \sum_{d \mid q} (0)^{q-d} = 1$, a contradiction.

(iii) This follows from the fact that the series $\sum_{1 < d \mid q} z^{2(d-1)} \left(\widetilde{X}_q(z)\right)^{d-1}$ is of order $2(p(q) - 1)$. □

The parity patterns $\widetilde{\Pi}_q$ also admit of an analogue of Theorem 3, which we describe next. For an odd integer $q \geq 3$ let $D(q) = \{d_0, d_1, \ldots, d_r\}$ be the set of divisors of q ordered in the natural way, so that $d_0 = 1$, $d_1 = p(q)$, and $d_r = q$. Form the vector

$$\underline{d}(q) = (d_1 - 1, \ldots, d_r - 1) \in \mathbb{N}^r.$$

For a vector $\underline{v} = (v_1, \ldots, v_r) \in \mathbb{N}_0^r$ we define its norm as $||\underline{v}|| = \sum_{i=1}^r v_i$, and if $\underline{v} = (v_1, \ldots, v_r)$ and $\underline{w} = (w_1, \ldots, w_r)$ are two such vectors, then their scalar product is given by $\underline{v} \cdot \underline{w} = \sum_{i=1}^r v_i w_i$. Denote the zero vector $(0, \ldots, 0)$ by $\underline{0}$, and for $i \in [r]$ let $\underline{e}_i$ be the i–th unit vector, i.e., the vector in $\mathbb{N}_0^r$ whose j–th component is δ_{ij}. A sequence $\underline{\underline{v}} = \{\underline{v}_k\}_0^\infty \in (\mathbb{N}_0^r)^{\mathbb{N}_0}$ is called *finitary* if there exists some $\mu \in \mathbb{N}_0$ such that $\underline{v}_k = \underline{0}$ for all $k > \mu$. The smallest such μ is called the *length* $\ell(\underline{\underline{v}})$ of $\underline{\underline{v}}$. The *$q$–norm* $||\underline{\underline{v}}||_q$ of a finitary sequence $\underline{\underline{v}} \in (\mathbb{N}_0^r)^{\mathbb{N}_0}$ is defined as

$$||\underline{\underline{v}}||_q := \sum_{k=0}^{\infty} \underline{v}_k \cdot \underline{d}(q).$$

For $r \in \mathbb{N}$ and $i \in [r]$ let

$$\mathcal{A}(i,r) := \Big\{ \underline{\underline{v}} \in (\mathbb{N}_0^r)^{\mathbb{N}_0} : \ \underline{\underline{v}} \text{ is finitary and } \underline{v}_0 = \underline{e}_i \Big\}.$$

Then we have the following explicit description of the parity pattern $\widetilde{\Pi}_q$.[13]

Theorem 8. *For every odd integer $q \geq 3$,*

$$\widetilde{\Pi}_q = \{1\} \cup \left\{ n \in \mathbb{N} - 2\mathbb{N} : \ \sum_{i=1}^{r} \sum_{\substack{\underline{\underline{v}} \in \mathcal{A}(i,r) \\ ||\underline{\underline{v}}||_q = \frac{n-1}{2}}} \prod_{k=0}^{\infty} \binom{\underline{v}_k \cdot \underline{d}(q)}{\underline{v}_{k+1}, \underline{v}_k \cdot \underline{d}(q) - ||\underline{v}_{k+1}||} \equiv 1 \mod 2 \right\}.$$

Proof. Using the identity (49) plus the multinomial law in $GF(2)[[z]]$, induction shows that for every $\mu \in \mathbb{N}_0$ we have the $GF(2)$–relation

$$\widetilde{X}_q(z) = 1 + \sum_{i=1}^{r} \sum_{\substack{\underline{\underline{v}} \in \mathcal{A}(i,r) \\ \ell(\underline{\underline{v}}) \leq \mu}} \prod_{k=0}^{\infty} \binom{\underline{v}_k \cdot \underline{d}(q)}{\underline{v}_{k+1}, \underline{v}_k \cdot \underline{d}(q) - ||\underline{v}_{k+1}||} z^{2||\underline{\underline{v}}||_q} + \widetilde{\mathcal{R}}_\mu(z),$$

where

$$\widetilde{\mathcal{R}}_\mu(z) := \sum_{i=1}^{r} \sum_{\underline{v}_1, \dots, \underline{v}_{\mu+1} \in \mathbb{N}_0^r \setminus \{\underline{0}\}} \binom{d_i - 1}{\underline{v}_1, d_i - 1 - ||\underline{v}_1||}$$

$$\times \prod_{k=1}^{\mu} \binom{\underline{v}_k \cdot \underline{d}(q)}{\underline{v}_{k+1}, \underline{v}_k \cdot \underline{d}(q) - ||\underline{v}_{k+1}||} z^{2(d_i - 1 + \sum_{k=1}^{\mu+1} \underline{v}_k \cdot \underline{d}(q))} \big(\widetilde{X}_q(z)\big)^{\underline{v}_{\mu+1} \cdot \underline{d}(q)}.$$

Proceeding as in the proof of Theorem 3 one then deduces that for every $\mu \geq 0$

$$\left|\left| \widetilde{X}_q(z) - \left[1 + \sum_{i=1}^{r} \sum_{\underline{\underline{v}} \in \mathcal{A}(i,r)} \prod_{k=0}^{\infty} \binom{\underline{v}_k \cdot \underline{d}(q)}{\underline{v}_{k+1}, \underline{v}_k \cdot \underline{d}(q) - ||\underline{v}_{k+1}||} z^{2||\underline{\underline{v}}||_q} \right] \right|\right| \leq 2^{-2(\mu+2)},$$

and, hence, letting $\mu \to \infty$ that

$$\widetilde{X}_q(z) = 1 + \sum_{m=1}^{\infty} \left(\sum_{i=1}^{r} \sum_{\substack{\underline{\underline{v}} \in \mathcal{A}(i,r) \\ ||\underline{\underline{v}}||_q = m}} \prod_{k=0}^{\infty} \binom{\underline{v}_k \cdot \underline{d}(q)}{\underline{v}_{k+1}, \underline{v}_k \cdot \underline{d}(q) - ||\underline{v}_{k+1}||} \right) z^{2m},$$

whence the theorem. $\square$

[13] We adhere to the convention that if $n, n_1, \dots, n_r$ are integers such that $n \geq 0$, $n_1 + \cdots + n_r = n$, and $n_k < 0$ for at least one $j \in [r]$, then the multinomial coefficient $\binom{n}{n_1, \dots, n_r}$ is defined and equal to zero.

We now come to the main result of this section. As is apparent from the previous theorem, the parity patterns $\widetilde{\Pi}_q$ with q odd will not in general lend themselves to a "nice" explicit characterization; indeed, as it turns out, the only exception occurs when q is a Fermat prime. For an integer $q \geq 3$ define

$$\Lambda_q := \left\{ \frac{2(q-1)^\sigma - q}{q-2} : \ \sigma = 1, 2, \dots \right\},$$

i.e., Λ_q is the set of partial sums of the series $1 + 2\sum_{\sigma=1}^\infty (q-1)^\sigma$.

Theorem 9. *Let $q \geq 3$ be an odd integer. Then the following assertions are equivalent:*

(i) $\widetilde{\Pi}_q = \Lambda_q$.

(ii) $\tilde{\chi}_q(n) = 0$ *for* $2 \leq n \leq 2q(q-1)$ *and* $n \neq 2q-1$.

(iii) q *is a Fermat prime.*

Proof. Since (i) clearly implies (ii), it suffices to prove the implications (ii)⇒(iii) and (iii)⇒(i). Assume first that q is not a Fermat prime. If q is not a prime, then $2 \leq 2p(q) - 1 < 2q - 1$, and we have observed before that for q odd $\tilde{\chi}_q(2p(q)-1) = 1$. Suppose on the other hand that q is a prime, and let

$$\nu_0 := \min \left\{ k \in [q-1] : \ \binom{q-1}{k} \equiv 1(2) \right\}.$$

Since q is not a Fermat prime, we certainly have $1 \leq \nu_0 < q-1$. Define $n_0 := 2(\nu_0+1)(q-1)$. Then $2q-1 < n_0 + 1 \leq 2q(q-1)$, and from (50), the fact that $\tilde{\chi}_q(2) = \cdots = \tilde{\chi}_q(2(q-1)) = 0$, and the definition of ν_0 we find that

$$\tilde{\chi}_q(n_0+1) = \sum_{\substack{\pi \vdash 2\nu_0(q-1) \\ ||\pi|| \leq q-1}} \binom{q-1}{||\pi||} \frac{||\pi||!}{\prod_{j=1}^\infty \pi_j!} \prod_{j=1}^\infty \big(\tilde{\chi}_q(j+1)\big)^{\pi_j} = \tilde{\chi}_q(2q-1) = 1.$$

In both cases we obtain a contradiction to (ii), thus proving the implication (ii)⇒(iii). Now suppose that q is a Fermat prime. Then (since q is a prime) the formula for $\widetilde{\Pi}_q$ given in Theorem 8 simplifies to

$$\widetilde{\Pi}_q = \{1\} \cup \left\{ n \in \mathbb{N} - 2\mathbb{N} : \sum_{\substack{\underline{\alpha} \in \mathcal{A} \\ 2(q-1)||\underline{\alpha}|| = n-1}} \prod_{k=0}^\infty \binom{\alpha_k(q-1)}{\alpha_{k+1}} \equiv 1 \mod 2 \right\} \tag{53}$$

in the notation of Theorem 3. Moreover, given a finitary sequence $\underline{\alpha} \in \mathcal{A}$, we will have $\prod_{k=0}^\infty \binom{\alpha_k(q-1)}{\alpha_{k+1}} \equiv 1(2)$ if and only if $\underline{\alpha}$ is of the form $\underline{\alpha} = (1, q-1, (q-1)^2, \dots, (q-1)^\sigma, 0, \dots)$ for some $\sigma \geq 0$. If $n \in \widetilde{\Pi}_q$, then by (53) either $n = 1$ or there exists some $\underline{\alpha} \in \mathcal{A}$ such that $2(q-1)||\alpha|| = n-1$ and $\prod_{k=0}^\infty \binom{\alpha_k(q-1)}{\alpha_{k+1}} \equiv 1(2)$. By the observation above this implies $n \in \Lambda_q$. Conversely, suppose that $n \in \Lambda_q$ and $n > 1$. Since $\frac{n-1}{2(q-1)}$ has a unique representation in base $q-1$, there exists precisely one finitary sequence $\underline{\alpha} \in \mathcal{A}$ with $2(q-1)||\underline{\alpha}|| = n-1$ and $\prod_{k=0}^\infty \binom{\alpha_k(q-1)}{\alpha_{k+1}} \equiv 1(2)$, and formula (53) implies that $n \in \widetilde{\Pi}_q$. Hence, $\widetilde{\Pi}_q = \Lambda_q$, proving the implication (iii)⇒(i). □

Remark 2. *Let $q \geq 3$ be an odd integer, but not a Fermat prime. Then, by the previous theorem, we have $\widetilde{\Pi}_q \neq \Lambda_q$ and, more precisely, there exists a deviation of $\widetilde{\Pi}_q$ from the pattern Λ_q within the set of integers $[2q(q-1)] - \{1, 2q-1\}$. In fact, our proof of the implication* (ii)$\Rightarrow$(iii) *of Theorem* 9 *yields a slightly sharper result. Let $n_q := \min_{n \in \widetilde{\Pi}_q \,\Delta\, \Lambda_q} n$, i.e., n_q is the smallest integer for which $\widetilde{\Pi}_q$ and Λ_q differ as to their containing or not containing this number. Then we have*

$$n_q = \begin{cases} 2(\nu_0+1)(q-1)+1, & q \text{ a prime} \\ 2p(q)-1, & \text{otherwise,} \end{cases} \tag{54}$$

where $\nu_0 = \min_{\binom{q-1}{k} \equiv 1(2),\, k \geq 1} k$. Furthermore, in the first case, i.e., q a prime but not a Fermat prime, we have $2 \leq \nu_0 < \frac{q-1}{2}$, which when combined with (54) *yields the estimate*

$$6q - 5 \;\leq\; n_q \;\leq\; (q-1)^2 + 1 \tag{55}$$

in terms of q alone. For $q = 7$ both these bounds are sharp.

Remark 3. *If $q \geq 3$ is odd but not a Fermat prime, the simplest instance of a parity pattern $\widetilde{\Pi}_q$ occurs when $q = 9$, this being the only odd integer $q > 1$, which is not a prime and has the property that each divisor $d > 1$ of q is such that $d - 1$ is a 2–power. The pattern $\widetilde{\Pi}_9$ can be described as follows. Define two linear operators Θ_1 and Θ_2 on the integers via $\Theta_1(a) = 2a + 3$ and $\Theta_2(b) = 8b + 9$. Then $\widetilde{\Pi}_9$ is the set of all positive integers, which can be obtained from* 1 *by applying Θ_1 and Θ_2 independently a finite number of times; in particular, the elements of $\widetilde{\Pi}_9$ are canonically parametrized by the free semigroup of rank* 2 *with unit element.*

6. Square decomposition of subdiagonals and the series $\mathcal{R}_q^{\mu,\nu}(z)$

The proof of formula (48) – and hence that of its consequences Theorems 5–9 – given in the previous section rests on two statements of a rather technical nature, left unproven at that stage so as not to disrupt the discussion too much. These statements are: (i) formula (46) computing the quotients $\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z)$ modulo 2 in terms of the series $\widetilde{S}_q(z)$, and (ii) assumption (47) concerning the integrality of the series $\mathcal{R}_q^{\mu,\nu}(z)$. The purpose of this section is to establish these two facts, in this way completing the proofs of the results in Section 5. We begin by showing the following.

Lemma 4. *For every $\nu \in \mathbb{N}_0$ the series $\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z)$ is an integral power series, and satisfies the congruence* (46)*.*

Proof. Integrality of the series $\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z)$ is easy; for instance it follows trivially by induction on ν using the formula

$$\widetilde{H}_q^{(\nu+1)}(z)/\widetilde{H}_q(z) = \Big(\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z)\Big)' + \widetilde{S}_q(z)\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z), \quad \nu \geq 0,$$

which in turn is an immediate consequence of (44). However, this approach does not seem to lead to a straightforward proof of the congruence (46). The following argument, which in particular automatically detects (46), appears to be more natural. Rewrite (44) in the form $\widetilde{H}_q(z) = \exp\big(\int \widetilde{S}_q(z)\,dz\big)$ and apply Bells formula (17) to obtain

$$\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z) = \sum_{\pi\vdash\nu} \frac{\nu!}{\prod_{j=1}^\infty (j!)^{\pi_j}\,\pi_j!} \prod_{j=1}^\infty \Big(\widetilde{S}_q^{(j-1)}(z)\Big)^{\pi_j}, \quad \nu \geq 0. \tag{56}$$

The coefficients occurring in (56) have a natural combinatorial interpretation: For a partition π consider the set $\mathcal{M}(\pi)$ of all maps $[||\pi||] \to 2^{[|\pi|]}$, denoted by $i \mapsto N_i$, such that

(i) $N_i \cap N_j = \emptyset$ for $1 \leq i, j \leq ||\pi||$ and $i \neq j$,

(ii) $\bigcup_{i=1}^{||\pi||} N_i = [|\pi|]$,

(iii) $|N_{i_j}| = j$ for $i_j \in [\pi_j] + \sum_{k=1}^{j-1} \pi_k$ and all $j \geq 1$.

We have

$$|\mathcal{M}(\pi)| = |\pi|!/\prod_{j=1}^\infty (j!)^{\pi_j}.$$

Let $G(\pi)$ be the permutation group consisting of all permutations of $S_{||\pi||}$ leaving invariant the decomposition

$$[||\pi||] = \coprod_{j=1}^\infty \Big([\pi_j] + \textstyle\sum_{k=1}^{j=1} \pi_k\Big)$$

of $[||\pi||]$, and let $G(\pi)$ act (from the right say) on $\mathcal{M}(\pi)$ in the natural way. Clearly, this action of $G(\pi)$ on $\mathcal{M}(\pi)$ is free, and $G(\pi) \cong \prod_{j=1}^\infty S_{\pi_j}$. Hence,

$$\frac{|\pi|!}{\prod_{j=1}^\infty (j!)^{\pi_j}\,\pi_j!} = |\mathcal{M}(\pi)/G(\pi)|;$$

in particular these numbers are integers. Since the series $\widetilde{S}_q(z)$ is integral, our first claim follows from (56). Moreover, using the fact that $\widetilde{S}_q^{(\mu)}(z) \equiv 0\,(2)$ for $\mu \geq 2$, we have modulo 2

$$\begin{aligned}\widetilde{H}_q^{(\nu)}(z)/\widetilde{H}_q(z) &\equiv \sum_{\substack{\pi\vdash\nu\\ \pi_j=0\,(j>2)}} \frac{\nu!}{\prod_{j=1}^\infty (j!)^{\pi_j}\,\pi_j!} \prod_{j=1}^\infty \Big(\widetilde{S}_q^{(j-1)}(z)\Big)^{\pi_j}\\ &\equiv \sum_{\mu=0}^{\lfloor\nu/2\rfloor} \binom{\nu}{2\mu} \big(\widetilde{S}_q'(z)\big)^\mu \big(\widetilde{S}_q(z)\big)^{\nu-2\mu},\end{aligned}$$

which is (46). $\square$

We now come to the main topic of this section, namely the verification of assumption (47) concerning the integrality of the series $\mathcal{R}_q^{\mu,\nu}(z)$. Given any $q \geq 3$, define a system of polynomials $\mathfrak{p}_q^{\ell,\mu}(t) \in \mathbb{Z}[t]$ indexed by two extra parameters $\ell \in \mathbb{Z}$ and $\mu \in \mathbb{N}_0$ via the equations

$$\mathfrak{p}_q^{\ell,0}(t) = \delta_{\ell,0} \quad (\ell \in \mathbb{Z}), \tag{57}$$

$$\mathfrak{p}_q^{\ell,\mu}(t) = 0 \quad (\ell < 0,\ \mu > 0), \tag{58}$$

$$\mathfrak{p}_q^{\ell,\mu}(t) = \sum_{\substack{d|q\\ d\leq\mu}} (t+\mu-1)_{d-1}\, \mathfrak{p}_q^{\ell,\mu-d}(t) \;+\; \sum_{\substack{d|q\\ d>\mu}} (t+\mu-1)_{\mu-1}\, \mathfrak{p}_q^{\ell+\mu-d,d-\mu}(t+\mu-d)$$
$$(\ell\geq 0,\;\; \mu>0). \tag{59}$$

An immediate induction on ℓ, followed by induction on μ, shows that (57) – (59) uniquely define a system $\big\{\mathfrak{p}_q^{\ell,\mu}(t)\big\}_{(q,\ell,\mu)}$ of integral polynomials parametrized by the triples

$$(q,\ell,\mu)\in \big(\mathbb{N}-\{1,2\}\big)\times\mathbb{Z}\times\mathbb{N}_0.$$

As our next result shows, these polynomials $\mathfrak{p}_q^{\ell,\mu}(t)$, for every $q\geq 3$, relate the subdiagonals of the array $\big(h_\mu(q)\, h_\nu(q)\big)_{\mu,\nu\geq 0}$ to the terms of its main diagonal. It is this important observation which underlies our proof of hypothesis (47).

Lemma 5. *For every $q\geq 3$, $\mu\geq 0$, and $n\geq 0$, and with $\mathfrak{p}_q^{\ell,\mu}(t)$ as defined above, we have*

$$h_n(q)\, h_{n+\mu}(q) = \sum_{\ell=0}^{n} \mathfrak{p}_q^{\ell,\mu}(n)\, (n)_\ell\, h_{n-\ell}^2(q). \tag{60}$$

Proof. We will fix $q\geq 3$, and prove (60) for all $\mu, n\geq 0$ by induction on n, followed by induction on μ. Suppose first that $n=0$. In this case we have to show that

$$h_\mu(q) = \mathfrak{p}_q^{0,\mu}(0),\quad \mu\geq 0. \tag{61}$$

This holds for $\mu=0$ in view of (57). Fix an integer $M>0$, and assume that (61) holds for all μ such that $0\leq\mu<M$. Then, by (42), our inductive hypothesis, (58), and (59) with $\mu=M$ and $\ell=t=0$

$$h_M(q) = \sum_{\substack{d|q\\ d\leq M}} (M-1)_{d-1}\, h_{M-d}(q) = \sum_{\substack{d|q\\ d\leq M}} (M-1)_{d-1}\, \mathfrak{p}_q^{0,M-d}(0) = \mathfrak{p}_q^{0,M}(0).$$

Hence, (60) holds for $n=0$, all $\mu\geq 0$, and $q\geq 3$ as fixed above. Now let $N>0$ be an integer, and suppose that (60) holds for all n with $0\leq n<N$, all $\mu\geq 0$, and our fixed value of q. In order to complete the induction step for our induction on n, we have to show that

$$h_N(q)\, h_{N+\mu}(q) = \sum_{\ell=0}^{N} \mathfrak{p}_q^{\ell,\mu}(N)\, (N)_\ell\, h_{N-\ell}^2(q) \tag{62}$$

holds for all $\mu\geq 0$. To see this we proceed again by induction on μ. In view of (57), (62) is true for $\mu=0$. Suppose then that (62) holds true for all μ with $0\leq\mu<M$ and some positive integer M. Then, by (42), the inductive hypotheses, (58), and (59) with

$\mu = M$ and $t = N$

$$h_N(q)\, h_{N+M}(q) = \sum_{d\mid q} (N+M-1)_{d-1}\, h_N(q)\, h_{N+M-d}(q)$$

$$= \sum_{\substack{d\mid q\\ d\leq M}} (N+M-1)_{d-1} \sum_{\ell=0}^{N} \mathfrak{p}_q^{\ell,M-d}(N)\,(N)_\ell\, h_{N-\ell}^2(q)$$

$$+ \sum_{\substack{d\mid q\\ M<d\leq N+M}} (N+M-1)_{d-1} \sum_{\ell=0}^{N+M-d} \mathfrak{p}_q^{\ell,d-M}(N+M-d)\,(N+M-d)_\ell\, h_{N+M-d-\ell}^2(q)$$

$$= \sum_{\ell=0}^{N} \Bigg[\sum_{\substack{d\mid q\\ d\leq M}} (N+M-1)_{d-1}\, \mathfrak{p}_q^{\ell,M-d}(N)$$

$$+ \sum_{\substack{d\mid q\\ d>M}} (N+M-1)_{M-1}\, \mathfrak{p}_q^{\ell+M-d,d-M}(N+M-d) \Bigg] (N)_\ell\, h_{N-\ell}^2(q)$$

$$= \sum_{\ell=0}^{N} \mathfrak{p}_q^{\ell,M}(N)\,(N)_\ell\, h_{N-\ell}^2(q).$$

This completes the proof of (62), and hence of the lemma. □

We now come to the main result of this section.

Proposition 3. *For every $(q,\mu,\nu) \in (\mathbb{N} - \{1,2\}) \times \mathbb{N} \times \mathbb{N}_0$, the series $\mathcal{R}_q^{\mu,\nu}(z)$ is an integral power series; in particular, assumption (47) holds true.*

Proof. With the convention that the zero polynomial has degree -1, decompose each $\mathfrak{p}_q^{\ell,\mu}(t)$ according to [22, Lemma 5] in the form

$$\mathfrak{p}_q^{\ell,\mu}(t) = \sum_{\kappa=0}^{d_q^{\ell,\mu}} a_q^{\ell,\mu}(\kappa)\,(t)_\kappa, \quad (q,\ell,\mu) \in (\mathbb{N} - \{1,2\}) \times \mathbb{Z} \times \mathbb{N}_0, \tag{63}$$

where $\deg\big(\mathfrak{p}_q^{\ell,\mu}(t)\big) = d_q^{\ell,\mu}$, and with $a_q^{\ell,\mu}(\kappa) \in \mathbb{Z}$ for all q, ℓ, μ, and κ. Then, by Lemma 5 and (63), we have for $q \geq 3$, $\mu > 0$, and $\nu \geq 0$ that

$$\begin{aligned}\sum_{n=0}^{\infty} h_n(q)\, h_{n+\mu}(q)\, z^n/n! &= \sum_{n=0}^{\infty} \sum_{\ell=0}^{n} \sum_{\kappa=0}^{d_q^{\ell,\mu}} a_q^{\ell,\mu}(\kappa)\, (n)_\kappa\, (n)_\ell\, h_{n-\ell}^2(q)\, z^n/n! \\ &= \sum_{\ell=0}^{\infty} \sum_{\kappa=0}^{d_q^{\ell,\mu}} a_q^{\ell,\mu}(\kappa) \sum_{n=0}^{\infty} (n+\ell)_\kappa\, h_n^2(q)\, z^{n+\ell}/n! \\ &= \sum_{\ell=0}^{\infty} \sum_{\kappa=0}^{d_q^{\ell,\mu}} a_q^{\ell,\mu}(\kappa)\, z^\kappa \left(z^\ell\, \widetilde{H}_q(z)\right)^{(\kappa)}.\end{aligned}$$

Invoking Leibniz's formula and introducing the numbers

$$A_{\ell,i}^{q,\mu} := \sum_{\kappa=0}^{d_q^{\ell,\mu}} \binom{\kappa}{i} (\ell)_{\kappa-i}\, a_q^{\ell,\mu}(\kappa)$$

this becomes

$$\sum_{n=0}^{\infty} h_n(q)\, h_{n+\mu}(q)\, z^n/n! = \sum_{\ell=0}^{\infty} \sum_{i=0}^{\infty} A_{\ell,i}^{q,\mu}\, z^{\ell+i}\, \widetilde{H}_q^{(i)}(z).$$

Taking the ν-th derivative, applying Leibniz's formula again, and dividing throughout by the series $\widetilde{H}_q(z)$ then gives

$$\mathcal{R}_q^{\mu,\nu}(z) = \sum_{\ell=0}^{\infty} \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \binom{\nu}{j} (\ell+i)_{\nu-j}\, A_{\ell,i}^{q,\mu}\, z^{\ell+i+j-\nu}\, \widetilde{H}_q^{(i+j)}(z)/\widetilde{H}_q(z).$$

Since the coefficients $A_{\ell,i}^{q,\mu}$ are well–defined integers, the family of series

$$\left\{ \binom{\nu}{j} (\ell+i)_{\nu-j}\, A_{\ell,i}^{q,\mu}\, z^{\ell+i+j-\nu}\, \widetilde{H}_q^{(i+j)}(z)/\widetilde{H}_q(z) \right\}_{\ell,i,j}$$

is summable (because of the factor $z^{\ell+i+j-\nu}$), and the series $\widetilde{H}_q^{(i+j)}(z)/\widetilde{H}_q(z)$ are integral for all $i, j \geq 0$ by Lemma 4, we conclude that for every $q \geq 3$, $\mu > 0$, and $\nu \geq 0$ the remainder series $\mathcal{R}_q^{\mu,\nu}(z)$ is indeed integral, as claimed. □

With Lemma 4 and Proposition 3 in hand, the proof of formula (48), and hence of Theorems 5–9 is complete.

7. The parity pattern of a Hecke group

In this final section we establish a relationship between the parity pattern of an arbitrary group and that of one of its index 2 subgroups. Once established, this relationship will allow us in particular to translate the results obtained for the patterns $\widetilde{\Pi}_q$ into results concerning the parity patterns of Hecke groups.

7.1. **Index 2 descent.** As a rule, divisibility properties of subgroup counting functions (unlike their growth behaviour) tend to react extremely sensitively to movements within a commensurability class; in particular, when passing from a group to one of its finite index subgroups, arithmetic structure of this kind is usually severely deformed if not completely destroyed. The following result appears to be the one non–trivial exception to this rule.

Proposition 4. *Let $\mathfrak{G}$ be a group containing only finitely many subgroups of index n for every positive integer n, and let $\mathfrak{H}$ be a subgroup of index 2 in $\mathfrak{G}$. Then*

$$\Pi(\mathfrak{G}) = \Big(\Pi(\mathfrak{H}) \,\cap\, (\mathbb{N} - 2\mathbb{N})\Big) \,\cup\, 2\,\Pi(\mathfrak{H}). \tag{64}$$

Proof. Every subgroup $\mathfrak{G}'$ of index n in $\mathfrak{G}$, which is not contained in $\mathfrak{H}$, intersects $\mathfrak{H}$ in a subgroup $\mathfrak{H}'$ with $(\mathfrak{H}:\mathfrak{H}') = n$. Hence, each such $\mathfrak{G}'$ is contained in the set $\bigcup_{(\mathfrak{H}:\mathfrak{H}')=n} \mathfrak{S}(\mathfrak{H}')$, where

$$\mathfrak{S}(\mathfrak{H}') := \Big\{\mathfrak{G}' \leq \mathfrak{G} :\ \ \mathfrak{G}' \cap \mathfrak{H} = \mathfrak{H}' \ \text{ and } \ \mathfrak{G}'\mathfrak{H} = \mathfrak{G}\Big\},$$

and, conversely, each $\mathfrak{G}' \in \bigcup_{(\mathfrak{H}:\mathfrak{H}')=n} \mathfrak{S}(\mathfrak{H}')$ is of index n in $\mathfrak{G}$ and not contained in $\mathfrak{H}$. It follows that

$$s_n(\mathfrak{G}) = \sum_{(\mathfrak{H}:\mathfrak{H}')=n} |\mathfrak{S}(\mathfrak{H}')| \,+\, \begin{cases} s_{n/2}(\mathfrak{H}), & 2 \mid n \\ 0, & 2 \nmid n. \end{cases} \tag{65}$$

Fix an element ζ with $\mathfrak{G} = \langle \mathfrak{H}, \zeta\rangle$. Given a subgroup $\mathfrak{H}'$ of index n in $\mathfrak{H}$ and a right transversal $1 = \mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_n$ for $\mathfrak{H}'$ in $\mathfrak{H}$, then the elements $\mathfrak{g}_{\mu,\nu} := \mathfrak{h}_\mu \zeta^\nu$ with $(\mu,\nu) \in [n] \times \{0,1\}$ form a right transversal for $\mathfrak{H}'$ in $\mathfrak{G}$. A subgroup $\mathfrak{G}' \in \mathfrak{S}(\mathfrak{H}')$ must contain $\mathfrak{H}'$ as a subgroup of index 2, and an element $\mathfrak{g}_{\mu,1}$ for some μ. Hence, the sets

$$\mathfrak{G}'_\mu := \mathfrak{H}' \cup \mathfrak{H}'\mathfrak{g}_{\mu,1}, \quad \mu \in [n]$$

exhaust all possibilities for a subgroup $\mathfrak{G}' \in \mathfrak{S}(\mathfrak{H}')$. Clearly, such a set $\mathfrak{G}'_\mu$ is contained in $\mathfrak{S}(\mathfrak{H}')$ if and only if $\mathfrak{G}'_\mu$ is a subgroup of $\mathfrak{G}$. The necessary and sufficient condition for the latter to hold is that $\mathfrak{g}_{\mu,1}\mathfrak{H}'\mathfrak{g}_{\mu,1} = \mathfrak{H}'$, i.e., $\mathfrak{g}_{\mu,1}$ has to represent an involution in the group $N_{\mathfrak{G}}(\mathfrak{H}')/\mathfrak{H}'$. By a well–known theorem of Frobenius [9][14] if d divides the order of a finite group $\mathfrak{G}$, then the number of solutions in $\mathfrak{G}$ of the equation $x^d = 1$ is divisible by d. Applying this result with $d = 2$ to the group $N_{\mathfrak{G}}(\mathfrak{H}')/\mathfrak{H}'$ we see that $|N_{\mathfrak{G}}(\mathfrak{H}')/\mathfrak{H}'|$ is congruent modulo 2 to the number of solutions in $N_{\mathfrak{G}}(\mathfrak{H}')/\mathfrak{H}'$ of the equation $x^2 = 1$. Those among these solutions which are represented by elements $\mathfrak{g}_{\mu,0}$ constitute the totality of solutions of this equation in the subgroup $N_{\mathfrak{H}}(\mathfrak{H}')/\mathfrak{H}'$; hence, applying Frobenius' result again, their number is congruent modulo 2 to $|N_{\mathfrak{H}}(\mathfrak{H}')/\mathfrak{H}'|$. Thus,

$$|N_{\mathfrak{G}}(\mathfrak{H}')/\mathfrak{H}'| \equiv |N_{\mathfrak{H}}(\mathfrak{H}')/\mathfrak{H}'| \,+\, |\mathfrak{S}(\mathfrak{H}')| \bmod 2. \tag{66}$$

[14] See also [17].

It follows from (66) that $|\mathfrak{S}(\mathfrak{H}')|$ is odd if and only if $(N_{\mathfrak{G}}(\mathfrak{H}') : \mathfrak{H}') \equiv 0\,(2)$ and $(N_{\mathfrak{H}}(\mathfrak{H}') : \mathfrak{H}') \equiv 1\,(2)$. Consequently, in view of this and equation (65)

$$s_n(\mathfrak{G}) \equiv |\Omega_n| + \begin{cases} s_{n/2}(\mathfrak{H}), & 2 \mid n \\ 0, & 2 \nmid n \end{cases} \mod 2, \tag{67}$$

where

$$\Omega_n := \Big\{ \mathfrak{H}' \leq \mathfrak{H} : \ (\mathfrak{H} : \mathfrak{H}') = n,\ (N_{\mathfrak{H}}(\mathfrak{H}') : \mathfrak{H}') \equiv 1\,(2),\ \text{and}\ (N_{\mathfrak{G}}(\mathfrak{H}') : \mathfrak{H}') \equiv 0\,(2) \Big\}.$$

Denote by $\mathfrak{U}_n(\mathfrak{H})$ the set of all index n subgroups in $\mathfrak{H}$. Since $\mathfrak{H}$ is normal in $\mathfrak{G}$, $\mathfrak{G}$ acts on $\mathfrak{U}_n(\mathfrak{H})$ by conjugation, and this action restricts to an action of $\mathfrak{G}$ (and hence of $\mathfrak{H}$) on the set Ω_n. Therefore, if n is even and $\mathfrak{H}' \in \Omega_n$, then $(\mathfrak{H} : N_{\mathfrak{H}}(\mathfrak{H}')) \equiv 0\,(2)$, and Ω_n decomposes into classes of even length under $\mathfrak{H}$. Hence, in this case $|\Omega_n| \equiv 0\,(2)$, and, by (67)

$$s_n(\mathfrak{G}) \equiv s_{n/2}(\mathfrak{H}) \bmod 2, \quad 2 \mid n. \tag{68}$$

Suppose on the other hand that n is odd, and consider the action of $\mathfrak{G}$ on the set

$$\mathfrak{U}_n(\mathfrak{H}) - \Omega_n = \Big\{ \mathfrak{H}' \leq \mathfrak{H} : \ (\mathfrak{H} : \mathfrak{H}') = n \ \text{and}\ (N_{\mathfrak{G}}(\mathfrak{H}') : \mathfrak{H}') \equiv 1\,(2) \Big\}.$$

Then, if $\mathfrak{H}' \in \mathfrak{U}_n(\mathfrak{H}) - \Omega_n$, we have $(\mathfrak{G} : N_{\mathfrak{G}}(\mathfrak{H}')) \equiv 0\,(2)$, i.e., $\mathfrak{U}_n(\mathfrak{H}) - \Omega_n$ decomposes into classes of even length under the action of $\mathfrak{G}$. Hence in this case

$$s_n(\mathfrak{H}) = |\mathfrak{U}_n(\mathfrak{H})| \equiv |\Omega_n| \bmod 2,$$

and by (67)

$$s_n(\mathfrak{G}) \equiv s_n(\mathfrak{H}) \bmod 2, \quad 2 \nmid n. \tag{69}$$

Statements (68) and (69) can be rephrased as

$$\Pi(\mathfrak{G}) \cap 2\,\mathbb{N} = 2\,\Pi(\mathfrak{H}) \tag{70}$$

respectively

$$\Pi(\mathfrak{G}) \cap (\mathbb{N} - 2\mathbb{N}) = \Pi(\mathfrak{H}) \cap (\mathbb{N} - 2\mathbb{N}). \tag{71}$$

Taking the union of (70) and (71) yields (64). □

As an illustration let $\mathfrak{G} = C_2^{*r}$ be the free product of $r \geq 2$ copies of the cyclic group of order 2. Then we have $m_{\mathfrak{G}} = 2$ and $\mu(\mathfrak{G}) = r - 1$, hence $\mathfrak{G}$ contains an index 2 subgroup which is free of rank $r - 1$. Since a finitely generated infinite free group has all its subgroup numbers odd,[15] we find from Proposition 4 that $\Pi(\mathfrak{G}) = \mathbb{N}$, i.e., $s_n(\mathfrak{G})$ is odd for all $n \geq 1$. This had been conjectured in [10], and proved for the case when $r \geq 4$ in a subsequent paper; cf. [11, Theorem 1].

[15] This follows immediately from M. Hall's recursion formula [15, Theorem 5.2].

7.2. **The parity patterns Π_q.** Denote by $\chi_q(n)$ the number $s_n(\mathfrak{H}(q))$ of index n subgroups in the Hecke group $\mathfrak{H}(q)$ considered modulo 2, let $X_q(z) := \sum_{n=0}^{\infty} \chi_q(n+1)\, z^n$ be the associated generating function, and let $\Pi_q := \Pi(\mathfrak{H}(q))$. Note that for every $q \geq 3$ the group $\mathfrak{H}(q)$ is a split extension of $\widetilde{\mathfrak{H}}(q)$ by C_2; indeed, if $\mathfrak{H}(q) = \langle \sigma, \tau | \sigma^2 = \tau^q = 1\rangle$, then the subgroup generated by τ and τ^σ is isomorphic to $\widetilde{\mathfrak{H}}(q)$ with transversal $\{1, \sigma\}$. Hence, Proposition 4 applies to the effect that (i) for q even $\Pi_q = \mathbb{N}$ (by Theorem 5), and (ii) for q odd $\Pi_q = \widetilde{\Pi}_q \cup 2\,\widetilde{\Pi}_q$ (making use of Theorem 7(i)). Given the latter equation our results concerning the groups $\widetilde{\mathfrak{H}}(q)$ for q odd translate into results for Hecke groups, and we find the following.

Theorem 10. *Let $q \geq 3$ be an integer.*

(a) *If q is even, then $\Pi_q = \mathbb{N}$.*

(b) *If q is odd, then*

   (i) *the set Π_q is infinite,*

   (ii) *the first entries of Π_q are 1, 2, and $2p(q) - 1$,*

   (iii) *we have $X_q(z) = \widetilde{X}_q(z) + z\widetilde{X}_q(z^2)$.*

Theorem 11. *Let $q_1, q_2 \geq 3$ be odd integers, and suppose that $\Pi_{q_1} = \Pi_{q_2}$. Then we have $q_1 = q_2$.*

Theorem 12. *Let $q \geq 3$ be odd, and let $1 + r = \sigma_0(q)$ be the number of divisors of q. Then we have*[16]

$$\Pi_q = \big\{1, 2\big\} \cup \Theta_q \cup 2\,\Theta_q,$$

where

$$\Theta_q = \left\{ n \in \mathbb{N} - 2\,\mathbb{N} : \sum_{i=1}^{r} \sum_{\substack{\underline{\underline{v}} \in \mathcal{A}(i,r) \\ ||\underline{\underline{v}}||_q = \frac{n-1}{q}}} \prod_{k=0}^{\infty} \binom{\underline{v}_k \cdot \underline{d}(q)}{\underline{v}_{k+1},\, \underline{v}_k \cdot \underline{d}(q) - ||\underline{v}_{k+1}||} \equiv 1 \mod 2 \right\}.$$

Theorem 13. *Let $q \geq 3$ be an odd integer. Then the following assertions are equivalent:*

(i) $\Pi_q = \Lambda_q \cup 2\,\Lambda_q$.

(ii) *$\chi_q(n) = 0$ for n odd and $n \in [2q(q-1)] - \{1, 2q-1\}$.*

(iii) *q is a Fermat prime.*

If we restrict Theorem 13 to the case when q is a prime, then, in the light of Remark 2, we can be slightly more precise.

Corollary 2. *Let $q \geq 3$ be a prime. Then the following assertions are equivalent:*

(i) $\Pi_q = \Lambda_q \cup 2\,\Lambda_q$.

(ii) *$\chi_q(n) = 0$ for $n = 2\nu(q-1) + 1$ and $3 \leq \nu \leq \frac{q-1}{2}$.*

(iii) *q is a Fermat prime.*

---

[16] We use the notation of Theorem 8.

References

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

[2] P. J. Cameron, *Combinatorics*, Cambridge University Press, 1994.

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

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

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

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

[7] M. du Sautoy, Finitely generated groups, p–adic analytic groups and Poincaré series, *Ann. of Math.* **137** (1993), 639–670.

[8] M. du Sautoy and F. Grunewald, Analytic properties of zeta functions and subgroup growth, *Ann. of Math.*, submitted.

[9] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, *Berl. Sitz.* (1903), 987–991.

[10] M. Grady and M. Newman, Counting subgroups of given index in Hecke groups, Contemporary Mathematics Vol. 143, Am. Math. Society, 1993, 431–436.

[11] M. Grady and M. Newman, Some divisibility properties of the subgroup counting function for free products, *Math. Comp.* **58** (1992), 347–353.

[12] C. D. Godsil, *Algebraic Combinatorics*, Chapman & Hall, New York, 1993.

[13] M. Gromov, Groups of polynomial growth and expanding maps, *Publ. Math. IHES* **53** (1981), 53–78.

[14] M. Hall, Coset representations in free groups, *Trans. Amer. Math. Soc.* **67** (1949), 421–432.

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

[16] M. Hall and T. Radó, On Schreier systems in free groups, *Trans. Amer. Math. Soc,* **64** (1948), 386–408.

[17] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* **40** (1936), 468–501.

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

[19] A. Lubotzky, *Subgroup growth*, lecture notes prepared for the conference Groups '93 Galway/St. Andrews, University College, Galway.

[20] A. Lubotzky, Counting finite index subgroups, *Proceedings of the conference Groups '93 Galway/St. Andrews*, 368–404.

[21] A. Meyer, Divisibility properties of subgroup counting functions associated with finitely generated virtually free groups, PhD thesis, University of Bielefeld, 1998.

[22] T. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.

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

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

[25] T. Müller, Combinatorial classification of finitely generated virtually free groups, *J. Algebra* **195** (1997), 285–294.

[26] T. Müller, Enumerating representations in finite wreath products, *Adv. in Math.*, to appear.

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

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

[29] T. Müller, Remarks on the PhD thesis of A. Meyer, unpublished manuscript, 1998.

[30] O. Schreier, die Untergruppen der freien Gruppen, *Abh. Math. Sem. Univ. Hamburg* **5** (1927), 161–183.

[31] J.–P. Serre, *Trees*, Berlin–Heidelberg–New York, 1980.

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

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

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

[35] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, D. van Nostrand, Princeton, 1960.

School of Mathematical Sciences
Queen Mary and Westfield College
Mile End Road
London E1 4NS
England
E-mail: T.W.Muller@qmw.ac.uk