MODULAR ARITHMETIC OF FREE SUBGROUPS

Thomas W. Müller and Jan-Christoph Schlage-Puchta

1. Introduction

A group $\mathfrak{G}$ is *virtually free*, if it contains a free subgroup of finite index, or, equivalently,[1] if it is the fundamental group of a (connected) graph of finite groups of bounded order. For a finitely generated virtually free group $\mathfrak{G}$ (that is, the fundamental group of a finite graph of finite groups), denote by $f_\lambda(\mathfrak{G})$ the number of free subgroups of index $\lambda m_\mathfrak{G}$ in $\mathfrak{G}$, where $m_\mathfrak{G}$ denotes the least common multiple of the orders of the finite subgroups in $\mathfrak{G}$. The present paper is concerned with the behaviour modulo p of $f_\lambda(\mathfrak{G})$, where $\mathfrak{G}$ is as above and p is a prime dividing $m_\mathfrak{G}$.

Over the years, the sequence $f_\lambda(\mathfrak{G})$ has been subject to a fair amount of study; cf. for instance [9], [10], [16], [18], [20], [34], [35]. Today, the asymptotics and growth behaviour of the function $f_\lambda(\mathfrak{G})$ are well understood, as is its precise connection with the structure of $\mathfrak{G}$; for instance, it is shown in [16] that, for $\chi(\mathfrak{G}) < 0$,

$$f_\lambda(\mathfrak{G}) \sim K_\mathfrak{G} \left(\frac{m_\mathfrak{G}\lambda}{e}\right)^{-m_\mathfrak{G}\chi(\mathfrak{G})\lambda} \lambda^{1+\frac{|E|-|V|}{2}} \quad (\lambda \to \infty),$$

where

$$K_\mathfrak{G} = m_\mathfrak{G} \sqrt{(2\pi m_\mathfrak{G})^{|E|-|V|} \prod_{v\in V} |\mathfrak{G}(v)| / \prod_{e\in E} |\mathfrak{G}(e)|}.$$

Here, $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-), X)$ is a decomposition of $\mathfrak{G}$ in terms of a finite graph of finite groups, and V, E denote, respectively, the set of vertices and (geometric) edges of X. Parallel to these investigations, other subgroup counting functions have been studied over the last two decades, most notably the number $s_n(\mathfrak{G})$ of index n subgroups in a finitely generated group $\mathfrak{G}$; in particular, building on asymptotic machinery for the coefficients of entire functions of finite genus developed in [21], growth and asymptotic behaviour of $s_n(\mathfrak{G})$ have been determined in [19] for the case of a free product

$$\mathfrak{G} = G_1 * G_2 * \cdots * G_s * F_r$$

with finite groups G_σ.[2]

On the other hand, apart from some isolated results for certain individual groups (for instance the modular groups $PSL_2(\mathbb{Z})$ and $SL_2(\mathbb{Z})$), very little was known until recently

[1] This equivalence is known as the *structure theorem* for virtually free groups. It was proved in the finitely generated case by Karrass, Pietrowski, and Solitar [11], building heavily on the work of Stallings [32] on groups with infinitely many ends. The countably generated case was established by Cohen [3], while in its full generality the result is due to Scott [30].

[2] An exposition of these and other results concerning the function $s_n(\mathfrak{G})$ can be found in the forthcoming book [13] by Lubotzky and Segal.

concerning divisibility properties of the functions $f_\lambda(\mathfrak{G})$ and $s_n(\mathfrak{G})$.[3] The situation changed with the presentation of the papers [24], [25], and [28], and, at the time of writing, a substantial body of knowledge has formed, mostly concerning modular properties of the function $s_n(\mathfrak{G})$. These developments are surveyed in [27]. However, in contrast to the marked progress for the function $s_n(\mathfrak{G})$, results concerning divisibility properties of the function $f_\lambda(\mathfrak{G})$ are known so far only in the case where $p = 2$ and $\mathfrak{G} = \mathfrak{H}(q) \cong C_2 * C_q$ is a Hecke group for some $q \geq 3$; cf. [25, Sections 3–4] and [27, Section 6]. Indeed, extension of this theory of 'free parity patterns in Hecke groups' to a more substantial class of virtually free groups and a larger set of primes was posed as a problem in [27], and the present paper seeks to fill this gap.

Define the *type* $\tau(\mathfrak{G})$ of a finitely generated virtually free group $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-), X)$ 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

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

with V and E as above. We have $\zeta_\kappa(\mathfrak{G}) \geq 0$ for $\kappa < m_\mathfrak{G}$ and $\zeta_{m_\mathfrak{G}}(\mathfrak{G}) \geq -1$, with equality occurring in the latter inequality if and only if X is a tree; cf. [16, Lemma 2] and [17, Proposition 1]. It can be shown that the type $\tau(\mathfrak{G})$ is in fact an invariant of the group $\mathfrak{G}$, that is, independent of the particular decomposition of $\mathfrak{G}$ in terms of a graph of groups $(\mathfrak{G}(-), X)$, 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 positive integer n if and only if $\tau(\mathfrak{G}_1) = \tau(\mathfrak{G}_2)$; cf. [16, Theorem 2]. For a finitely generated virtually free group $\mathfrak{G}$ and a prime p define the *free rank* $\mu(\mathfrak{G})$ and the *p-rank* $\mu_p(\mathfrak{G})$ of $\mathfrak{G}$ by means of the formulae

$$\mu(\mathfrak{G}) = 1 + \sum_{\kappa \mid m_\mathfrak{G}} \varphi(m_\mathfrak{G}/\kappa)\zeta_\kappa(\mathfrak{G}) \tag{1}$$

respectively

$$\mu_p(\mathfrak{G}) = 1 + \sum_{p \mid \kappa \mid m_\mathfrak{G}} \varphi(m_\mathfrak{G}/\kappa)\zeta_\kappa(\mathfrak{G}), \tag{2}$$

where φ is Euler's totient function. The free rank $\mu(\mathfrak{G})$ as defined above in terms of the type $\tau(\mathfrak{G})$ turns out to coincide with the rank of a free subgroup of index $m_\mathfrak{G}$ in $\mathfrak{G}$; see the beginning of Section 2. A combinatorial interpretation of the p-rank $\mu_p(\mathfrak{G})$ of $\mathfrak{G}$ occurs in Section 3, in the proof of Lemma 1. Having given these definitions, we can now state our main results.

Theorem A. *Let $\mathfrak{G}$, $\mathfrak{G}_1$, $\mathfrak{G}_2$ be finitely generated virtually free groups, and let p be a prime dividing $m_\mathfrak{G}$, $m_{\mathfrak{G}_1}$, $m_{\mathfrak{G}_2}$.*

(i) *If $\mu_p(\mathfrak{G}) > 0$, then $f_\lambda(\mathfrak{G}) \equiv 0 \bmod p$ for all $\lambda \geq 1$.*

(ii) *If $\mu_p(\mathfrak{G}_1) = \mu_p(\mathfrak{G}_2) = 0$, then we have $f_\lambda(\mathfrak{G}_1) \equiv f_\lambda(\mathfrak{G}_2) \bmod p$ for all $\lambda \geq 1$ if and only if $\mu(\mathfrak{G}_1) = \mu(\mathfrak{G}_2)$.*

[3] Cf. [6], [7], [8], [15, Satz 2], [16, Proposition 6], [22], [34], or the introduction of [27] for results in this direction obtained prior to and including 1998.

(iii) *Suppose that* $\mu_p(\mathfrak{G}) = 0$. *Then the generating function* $\sum_\lambda f_\lambda(\mathfrak{G}) z^\lambda$ *is rational over* $GF(p)$ *if and only if* $\mu(\mathfrak{G}) = 0$, *or* $\mu(\mathfrak{G}) = 1$ *and* $p = 2$; *in particular, the set*

$$\mathcal{N}^{*p}(\mathfrak{G}) := \big\{\lambda \in \mathbb{N} :\ f_\lambda(\mathfrak{G}) \not\equiv 0 \bmod p\big\}$$

is infinite, provided that $\mu_p(\mathfrak{G}) = 0$ *and* $\mu(\mathfrak{G}) \geq 1$.

(iv) *Suppose that* $\mu_p(\mathfrak{G}) = 0$ *and that* $\mu(\mathfrak{G}) \geq 1$. *Then every entry of* $\mathcal{N}^{*p}(\mathfrak{G})$ *is congruent to* 1 *modulo* $(p-1)p^{\nu_p(\mu(\mathfrak{G}))}$; *moreover, the first two entries of* $\mathcal{N}^{*p}(\mathfrak{G})$ *are* 1 *and* $\alpha_{\mathfrak{G}}^{*p} = 1 + (p-1)p^{\nu_p(\mu(\mathfrak{G}))}$, *and we have*[4]

$$\begin{aligned} f_1(\mathfrak{G}) &\equiv (-1)^{\frac{\mu(\mathfrak{G})}{p-1}} \bmod p, \\ f_{\alpha_{\mathfrak{G}}^{*p}}(\mathfrak{G}) &\equiv (-1)^{\frac{\mu(\mathfrak{G})}{p-1}-1} \big\langle p^{\nu_p(\mu(\mathfrak{G}))} \mid \mu(\mathfrak{G})/(p-1) \big\rangle \bmod p. \end{aligned}$$

Here, $\nu_p(x)$ denotes the p-adic norm of x, that is, the exponent of p in the prime decomposition of x.

Theorem B. *Let* $\mathfrak{G}$ *and* p *be as in Theorem* A, *and suppose that* $\mu_p(\mathfrak{G}) = 0$.

(i) *For* $\lambda \geq 1$, *the function* $f_\lambda(\mathfrak{G})$ *satisfies the congruence*

$$f_\lambda(\mathfrak{G}) \equiv (-1)^{\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}} \lambda^{-1} \binom{\frac{\mu(\mathfrak{G})\lambda}{p-1}}{\frac{\lambda-1}{p-1}} \mod p.$$

(ii) *We have*

$$\mathcal{N}^{*p}(\mathfrak{G}) = \Big\{\lambda \in \mathbb{N} :\ \mathfrak{s}_p\Big(\frac{\lambda-1}{p-1}\Big) + \mathfrak{s}_p\Big(\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}\Big) - \mathfrak{s}_p\Big(\frac{\mu(\mathfrak{G})\lambda}{p-1}\Big) - \mathfrak{s}_p(\lambda-1) + \mathfrak{s}_p(\lambda) = 1\Big\}.$$

Here, $\mathfrak{s}_p(x)$ denotes the sum of digits in the p-adic expansion of x. Furthermore, throughout this paper, we use the convention that a binomial coefficient $\binom{\alpha}{n}$ equals zero if $n \notin \mathbb{N}_0$.

Theorem C. *Let* $\mathfrak{G}$ *and* p *be as in Theorem* A, *and suppose that* $\mu_p(\mathfrak{G}) = 0$ *and that* $\mu(\mathfrak{G}) \geq 2$. *Then the following assertions are equivalent:*

(i) $\mathcal{N}^{*p}(\mathfrak{G}) = \Big\{\dfrac{((p-1)\mu(\mathfrak{G}))^\sigma - 1}{(p-1)\mu(\mathfrak{G}) - 1} :\ \sigma = 1, 2, \dots\Big\}$.

(ii) $f_\lambda(\mathfrak{G}) \equiv 0 \bmod p$ *for* $2 \leq \lambda \leq (p-1)\mu(\mathfrak{G})$.

(iii) $\mu(\mathfrak{G})$ *is a 2-power, and* $p = 2$.

A few comments on Theorems A–C are in order. Theorem A collects together a miscellany of information concerning the function $f_\lambda(\mathfrak{G})$. Part (i) allows us to restrict attention to the case where $\mu_p(\mathfrak{G}) = 0$, while part (ii) states that for such groups $\mathfrak{G}$ the mod p behaviour of $f_\lambda(\mathfrak{G})$ is precisely classified by the free rank $\mu(\mathfrak{G})$. Part (iv)

[4]For a power series $f(z)$ and a non-negative integer n, we denote by $\langle z^n \mid f(z)\rangle$ the coefficient of z^n in $f(z)$. Here, the expansion of $\mu(\mathfrak{G})/(p-1)$ to base p is interpreted as a formal power series in p.

describes an interesting divisibility property of the set $\mathcal{N}^{*p}(\mathfrak{G})$, while part (iii) settles the question when the series $\sum_\lambda f_\lambda(\mathfrak{G})z^\lambda$ is rational over $GF(p)$: apart from the trivial case where $\mu_p(\mathfrak{G}) > 0$, this happens if and only if $\mathfrak{G}$ is finite of order divisible by p, or $\mathfrak{G} \cong G_1 *_S G_2$ with finite groups G_i, S of odd order, $(G_1 : S) = (G_2 : S) = 2$, and $p = 2$. Theorem B provides a surprisingly explicit combinatorial description of $f_\lambda(\mathfrak{G})$ and $\mathcal{N}^{*p}(\mathfrak{G})$. As is apparent from this description, the sets $\mathcal{N}^{*p}(\mathfrak{G})$ with $\mu_p(\mathfrak{G}) = 0$ will in general not lend themselves to a characterization in closed form as in the case of the modular groups; instead, $\mathcal{N}^{*p}(\mathfrak{G})$ generically tends to inherit the well-known kind of fractal behaviour observed in Pascal's triangle when evaluated modulo a prime. There is however one special case where we can describe the sets $\mathcal{N}^{*p}(\mathfrak{G})$ in a completely explicit way; this is the subject matter of Theorem C, which provides an optimal generalization of Stothers' formula for the parity of $f_\lambda(PSL_2(\mathbb{Z}))$; cf. [34]. As is well known, Fermat primes, that is, 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,[5] 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 C to the case where $p = 2$ and $\mathfrak{G} = \mathfrak{H}(q)$ is a Hecke group for some prime $q \geq 3$, we obtain a new such characterization in terms of the free parity pattern of the associated Hecke group.

Corollary C′. *Let $q > 2$ be a prime number. Then q is a Fermat prime if and only if*

$$f_\lambda(\mathfrak{H}(q)) \equiv 1 \bmod 2 \Longleftrightarrow \lambda = \frac{(q-1)^\sigma - 1}{q-2} \ \text{ for some } \ \sigma \geq 1.$$

The key to Theorems A–C is the functional equation

$$X^{*p}_{\mathfrak{G}}(z) = z\big(X^{*p}_{\mathfrak{G}}(z)\big)^{\mu_p(\mathfrak{G})}\Big(\big(X^{*p}_{\mathfrak{G}}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}, \quad p \mid m_{\mathfrak{G}} \tag{3}$$

for the mod p projection $X^{*p}_{\mathfrak{G}}(z)$ of the generating function $\sum_\lambda f_\lambda(\mathfrak{G})z^\lambda$, whose proof occupies Sections 2–5. In Sections 6 and 7 we exploit identity (3) to obtain the results described above concerning the mod p behaviour of the function $f_\lambda(\mathfrak{G})$; the contents of Theorem A is the subject matter of Section 6, while Section 7 deals with Theorems B and C. Part of the proof of Theorem B consists in the construction of a canonical lifting $\hat{X}^{*p}_{\mathfrak{G}}(z) \in \mathbb{Z}[[z]]$ for the $GF(p)$-series $X^{*p}_{\mathfrak{G}}(z)$, and the paper concludes with a number of combinatorial interpretations for the coefficients of $\hat{X}^{*p}_{\mathfrak{G}}(z)$ in the case where $p = 2$ and $\mu(\mathfrak{G}) \geq 2$.

2. A recurrence relation for $f_\lambda(\mathfrak{G})$

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 [16, formulae (3) and (9)]. Observe that $\mu(\mathfrak{G})$ is connected with the Euler characteristic of $\mathfrak{G}$ via

$$\mu(\mathfrak{G}) \ + \ m_{\mathfrak{G}}\chi(\mathfrak{G}) = 1, \tag{4}$$

[5] Disquisitiones Arithmeticae, § 366.

which shows in particular that $\mu(\mathfrak{G})$ is well–defined. The Euler characteristic of $\mathfrak{G}$ in turn can be expressed in terms of the type $\tau(\mathfrak{G})$ via

$$\chi(\mathfrak{G}) = -m_{\mathfrak{G}}^{-1} \sum_{\kappa | m_{\mathfrak{G}}} \varphi(m_{\mathfrak{G}}/\kappa)\, \zeta_\kappa(\mathfrak{G}). \tag{5}$$

Indeed,

$$\begin{aligned} \sum_{\kappa | m_{\mathfrak{G}}} \varphi(m_{\mathfrak{G}}/\kappa)\zeta_\kappa(\mathfrak{G}) &= \sum_{k=1}^{m_{\mathfrak{G}}} \Big[\big|\{e \in E :\ |\mathfrak{G}(e)| \mid k\}\big| - \big|\{v \in V :\ |\mathfrak{G}(v)| \mid k\}\big| \Big] \\ &= \sum_{e \in E} \frac{m_{\mathfrak{G}}}{|\mathfrak{G}(e)|} \ - \sum_{v \in V} \frac{m_{\mathfrak{G}}}{|\mathfrak{G}(v)|} = -m_{\mathfrak{G}}\, \chi(\mathfrak{G}), \end{aligned}$$

the last equality coming from the fact that the Euler characteristic $\chi(\mathfrak{G})$ in the sense of Wall coincides with the equivariant Euler characteristic $\chi_{\tilde{X}}(\mathfrak{G})$ relative to the tree $\tilde{X}$ associated with $\mathfrak{G}$ in the sense of Bass and Serre; cf., for example, [1, Chapter IX, Proposition 7.3]. Equations (4) and (5) imply in particular that, if two virtually free groups have the same number of free index n subgroups for each n, then their Euler characteristics and free ranks must coincide. The following result will be the starting point of our investigation.

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

$$f_{\lambda+1}(\mathfrak{G}) \ = \sum_{\mu=1}^{\mu(\mathfrak{G})} \sum_{\substack{\lambda_1,\ldots,\lambda_\mu > 0 \\ \lambda_1+\cdots+\lambda_\mu = \lambda}} (\mu!\, m_{\mathfrak{G}}^{\mu})^{-1}\, \mathcal{F}_\mu^{(\mathfrak{G})}(\lambda_1,\ldots,\lambda_\mu) \prod_{j=1}^{\mu} f_{\lambda_j}(\mathfrak{G}) \qquad (\lambda \geq 1,\ f_1(\mathfrak{G}) = A_0(\mathfrak{G})) \tag{6}$$

with coefficients

$$\mathcal{F}_\mu^{(\mathfrak{G})}(\lambda_1,\ldots,\lambda_\mu) := \sum_{\nu=\mu}^{\mu(\mathfrak{G})} \vartheta_\nu(\mathfrak{G})\, F_{\mu,\nu}(\lambda_1,\ldots,\lambda_\mu),$$

where

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

and the integers $\vartheta_\mu(\mathfrak{G})$ are given in terms of the type $\tau(\mathfrak{G})$ via

$$\vartheta_\mu(\mathfrak{G}) = \frac{1}{\mu!} \sum_{j=0}^{\mu} (-1)^{\mu-j} \binom{\mu}{j} m_{\mathfrak{G}}\, (j+1) \prod_{\kappa | m_{\mathfrak{G}}} \prod_{\substack{1 \leq k \leq m_{\mathfrak{G}} \\ (m_{\mathfrak{G}},k) = \kappa}} (j m_{\mathfrak{G}} + k)^{\zeta_\kappa(\mathfrak{G})}, \quad 0 \leq \mu \leq \mu(\mathfrak{G}). \tag{7}$$

This is [25, Proposition 1]. However, since [26] has not yet appeared in print, we include the proof for the convenience of the reader.

Proof of Proposition 1. 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 $g_\lambda(\mathfrak{G})$ by the condition that

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

in particular $g_0(\mathfrak{G}) = 1$. Then the arithmetic functions $f_\lambda(\mathfrak{G})$ and $g_\lambda(\mathfrak{G})$ are related via the transformation formula[6]

$$\sum_{1 \le \mu \le \lambda} f_\mu(\mathfrak{G})\, g_{\lambda-\mu}(\mathfrak{G}) = m_{\mathfrak{G}}\, \lambda\, g_\lambda(\mathfrak{G}), \quad \lambda \ge 1. \tag{8}$$

Moreover, the generating function $\Theta_{\mathfrak{G}}(z) := \sum_{\lambda \ge 0} g_\lambda(\mathfrak{G}) z^\lambda$ is known to satisfy the homogeneous linear differential equation

$$\vartheta_0(\mathfrak{G})\, \Theta_{\mathfrak{G}}(z) \,+\, (\vartheta_1(\mathfrak{G})\, z - m_{\mathfrak{G}})\, \Theta'_{\mathfrak{G}}(z) \,+\, \sum_{\mu=2}^{\mu(\mathfrak{G})} \vartheta_\mu(\mathfrak{G})\, z^\mu\, \Theta^{(\mu)}_{\mathfrak{G}}(z) = 0 \tag{9}$$

of order $\mu(\mathfrak{G})$ with integral coefficients $\vartheta_\mu(\mathfrak{G})$ as defined in Proposition 1; cf. [16, Proposition 5]. In view of equation (8), the series

$$\Xi_{\mathfrak{G}}(z) := \sum_{\lambda \ge 0} f_{\lambda+1}(\mathfrak{G})\, z^\lambda$$

is related to $\Theta_{\mathfrak{G}}(z)$ via the identity

$$\Xi_{\mathfrak{G}}(z) = m_{\mathfrak{G}}\, \frac{d}{dz} \big(\log\, \Theta_{\mathfrak{G}}(z) \big). \tag{10}$$

Applying Bell's formula[7]

$$\frac{d^\mu}{dz^\mu} \alpha(\beta(z)) = \sum_{\pi \vdash \mu} \frac{\mu!}{\prod_{j \ge 1} \pi_j!} \left[\prod_{j \ge 1} \left(\frac{\beta^{(j)}(z)}{j!} \right)^{\pi_j} \right] \alpha^{(||\pi||)}(\beta(z)) \tag{11}$$

for the derivatives of a composite function with $\alpha(t) = e^t$ and $\beta(z) = m_{\mathfrak{G}}^{-1} \int \Xi_{\mathfrak{G}}(z)\, dz$, we find that

$$\Theta^{(\mu)}_{\mathfrak{G}}(z) = \mu!\, \Theta_{\mathfrak{G}}(z) \sum_{\nu=1}^{\mu} \sum_{\substack{\mu_1, \ldots, \mu_\nu > 0 \\ \mu_1 + \cdots + \mu_\nu = \mu}} (\nu!\, m_{\mathfrak{G}}^\nu)^{-1} \prod_{j=1}^{\nu} \frac{\Xi^{(\mu_j - 1)}_{\mathfrak{G}}(z)}{\mu_j!}, \quad \mu \ge 1.$$

Combining the latter identities for $1 \le \mu \le \mu(\mathfrak{G})$ with (9), we obtain the differential equation

$$\Xi_{\mathfrak{G}}(z) = \vartheta_0(\mathfrak{G}) \,+\, \sum_{\mu=1}^{\mu(\mathfrak{G})} \sum_{\nu=1}^{\mu} \sum_{\substack{\mu_1, \ldots, \mu_\nu > 0 \\ \mu_1 + \cdots + \mu_\nu = \mu}} \binom{\mu}{\mu_1, \ldots, \mu_\nu} (\nu!\, m_{\mathfrak{G}}^\nu)^{-1}\, \vartheta_\mu(\mathfrak{G})\, z^\mu \prod_{j=1}^{\nu} \Xi^{(\mu_j - 1)}_{\mathfrak{G}}(z) \tag{12}$$

for $\Xi_{\mathfrak{G}}(z)$, and Proposition 1 follows by comparing coefficients in (12). □

[6] Cf. [16, Corollary 1] or [5, Proposition 1]. See also [23] for a far reaching generalization of the latter result.

[7] See the beginning of Section 4 for the conventions concerning number partitions used in this paper.

3. A divisibility property of $\vartheta_\mu(\mathfrak{G})$

Our next result describes an important divisibility property of the numbers $\vartheta_\mu(\mathfrak{G})$ introduced in Proposition 1.

Lemma 1. *Let $\mathfrak{G}$ be a finitely generated virtually free group, and let p be a prime.*

(i) *For $0 \le \mu \le \mu(\mathfrak{G})$, the integer $\vartheta_\mu(\mathfrak{G})$ is divisible by $m_{\mathfrak{G}}^\mu$.*

(ii) *If $m_{\mathfrak{G}}$ is divisible by p, then*[8]

$$m_{\mathfrak{G}}^{-\mu}\vartheta_\mu(\mathfrak{G}) \equiv (-1)^{\frac{\mu(\mathfrak{G})-2\mu_p(\mathfrak{G})+\mu}{p-1}} \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\frac{\mu-\mu_p(\mathfrak{G})}{p-1}} \mod p.$$

Proof. (i) Let

$$K_{\mathfrak{G}} = \Big\{ \underbrace{1,\dots,1}_{\zeta_1'}, \dots, \underbrace{k,\dots,k}_{\zeta_k'}, \dots, \underbrace{m_{\mathfrak{G}},\dots,m_{\mathfrak{G}}}_{\zeta_{m_{\mathfrak{G}}}'} \Big\}$$

be the multiset consisting of all integers $1 \le k \le m_{\mathfrak{G}}$, where k is taken with multiplicity

$$\zeta_k' = \zeta_k'(\mathfrak{G}) := \begin{cases} \zeta_{(k,m_{\mathfrak{G}})}(\mathfrak{G}), & k < m_{\mathfrak{G}} \\ \zeta_{m_{\mathfrak{G}}}(\mathfrak{G}) + 1, & k = m_{\mathfrak{G}}. \end{cases}$$

In view of (1), this multiset has

$$\sum_{1\le k\le m_{\mathfrak{G}}} \zeta_k'(\mathfrak{G}) = \sum_{\substack{\kappa \mid m_{\mathfrak{G}} \\ \kappa < m_{\mathfrak{G}}}} \varphi(m_{\mathfrak{G}}/\kappa)\zeta_\kappa(\mathfrak{G}) \,+\, \zeta_{m_{\mathfrak{G}}}(\mathfrak{G}) \,+\, 1 = \mu(\mathfrak{G})$$

elements. Think of $K_{\mathfrak{G}}$ as being linearly ordered as indicated above, and denote this (strict) order by $\prec$. We have

$$\vartheta_\mu(\mathfrak{G}) = \frac{1}{\mu!}\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j}\prod_{k\in K_{\mathfrak{G}}}(jm_{\mathfrak{G}}+k), \quad 0 \le \mu \le \mu(\mathfrak{G}). \tag{13}$$

Also,

$$\prod_{k\in K_{\mathfrak{G}}}(jm_{\mathfrak{G}}+k) = \sum_{\nu=0}^{\mu(\mathfrak{G})}(jm_{\mathfrak{G}})^\nu \Bigg(\prod_{k\in K_{\mathfrak{G}}} k\Bigg)\Bigg(\sum_{\substack{k_1,\dots,k_\nu\in K_{\mathfrak{G}} \\ k_1\prec\cdots\prec k_\nu}} \frac{1}{k_1k_2\cdots k_\nu}\Bigg). \tag{14}$$

Inserting (14) into (13), interchanging summations, and using the fact that

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

[8]Recall the convention concerning binomial coefficients mentioned in the introduction.

is a Stirling number of the second kind, we find that

$$\vartheta_\mu(\mathfrak{G}) = m_{\mathfrak{G}}^{\mu}\left[\left(\prod_{k\in K_{\mathfrak{G}}} k\right)\left(\sum_{\substack{k_1,\ldots,k_\mu\in K_{\mathfrak{G}}\\ k_1\prec\cdots\prec k_\mu}}\frac{1}{k_1k_2\cdots k_\mu}\right)+\right.$$

$$\left.\sum_{\nu=\mu+1}^{\mu(\mathfrak{G})} m_{\mathfrak{G}}^{\nu-\mu}\,S(\nu,\mu)\left(\prod_{k\in K_{\mathfrak{G}}} k\right)\left(\sum_{\substack{k_1,\ldots,k_\nu\in K_{\mathfrak{G}}\\ k_1\prec\cdots\prec k_\nu}}\frac{1}{k_1k_2\cdots k_\nu}\right)\right].$$

This shows that $\vartheta_\mu(\mathfrak{G})$ is divisible by $m_{\mathfrak{G}}^{\mu}$ for all $0\le\mu\le\mu(\mathfrak{G})$.

(ii) Now assume that $p \mid m_{\mathfrak{G}}$. Then we infer from the previous equation that, for $0\le\mu\le\mu(\mathfrak{G})$,

$$m_{\mathfrak{G}}^{-\mu}\vartheta_\mu(\mathfrak{G}) \equiv \left(\prod_{k\in K_{\mathfrak{G}}} k\right)\left(\sum_{\substack{k_1,\ldots,k_\mu\in K_{\mathfrak{G}}\\ k_1\prec\cdots\prec k_\mu}}\frac{1}{k_1k_2\cdots k_\mu}\right) \mod p. \tag{15}$$

Moreover, we find that the multiset $K_{\mathfrak{G}}$ contains precisely

$$\sum_{\substack{1\le k\le m_{\mathfrak{G}}\\ p\mid k}}\zeta_k'(\mathfrak{G}) = \sum_{\substack{\kappa\mid m_{\mathfrak{G}}\\ \kappa<m_{\mathfrak{G}}\\ p\mid\kappa}}\varphi(m_{\mathfrak{G}}/\kappa)\zeta_\kappa(\mathfrak{G}) + \zeta_{m_{\mathfrak{G}}}(\mathfrak{G}) + 1 = \mu_p(\mathfrak{G})$$

numbers divisible by p. Next, we observe that, for $p \mid m_{\mathfrak{G}}$, the multisets

$$K_{\mathfrak{G},p}^{(i)} := \Big\{k\in K_{\mathfrak{G}} :\ k\equiv i \bmod p\Big\},\quad 0<i<p$$

all share the same cardinality. Indeed, for $0<i<p$,

$$\begin{aligned}
\sum_{\substack{1\le k\le m_{\mathfrak{G}}\\ k\equiv i\,(p)}}\zeta_k'(\mathfrak{G}) &= \sum_{\substack{1\le k\le m_{\mathfrak{G}}\\ k\equiv i\,(p)}}\zeta_{(k,m_{\mathfrak{G}})}(\mathfrak{G})\\
&= \sum_{p\nmid\kappa\mid m_{\mathfrak{G}}}\zeta_\kappa(\mathfrak{G})\sum_{\substack{1\le k\le m_{\mathfrak{G}}\\ (k,m_{\mathfrak{G}})=\kappa\\ k\equiv i\,(p)}}1\\
&= \sum_{p\nmid\kappa\mid m_{\mathfrak{G}}}\zeta_\kappa(\mathfrak{G})\sum_{\substack{1\le \ell\le m_{\mathfrak{G}}/\kappa\\ (\ell,m_{\mathfrak{G}}/\kappa)=1\\ \ell\equiv\kappa' i\,(p)}}1 \quad (\kappa\kappa'\equiv 1 \bmod p)\\
&= \frac{1}{p-1}\sum_{p\nmid\kappa\mid m_{\mathfrak{G}}}\varphi(m_{\mathfrak{G}}/\kappa)\,\zeta_\kappa(\mathfrak{G})\\
&= \frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1} =: \mu_0^{(p)}(\mathfrak{G}).
\end{aligned}$$

It follows that the multiset

$$K^+_{\mathfrak{G},p} := \Big\{ k \in K_{\mathfrak{G}} : \; k \not\equiv 0 \bmod p \Big\}$$

allows a decomposition

$$K^+_{\mathfrak{G},p} = \coprod_{j=1}^{\mu_0^{(p)}(\mathfrak{G})} X_j \tag{16}$$

with sets X_j satisfying[9]

$$|X_j| = p-1, \;\; X_j \equiv [p-1] \bmod p \quad (1 \le j \le \mu_0^{(p)}(\mathfrak{G}));$$

in particular, we conclude from Wilson's Theorem that

$$\prod_{k \in K^+_{\mathfrak{G},p}} k \equiv (-1)^{\mu_0^{(p)}(\mathfrak{G})} \mod p. \tag{17}$$

Putting $\mu' := \mu - \mu_p(\mathfrak{G})$, decomposition (16) in conjunction with (15) and (17) now yields

$$\begin{aligned} m_{\mathfrak{G}}^{-\mu} \vartheta_\mu(\mathfrak{G}) &\equiv \Bigg(\prod_{k \in K^+_{\mathfrak{G},p}} k \Bigg) \Bigg(\sum_{\substack{k_1,\ldots,k_{\mu'} \in K^+_{\mathfrak{G},p} \\ k_1 \prec \cdots \prec k_{\mu'}}} \frac{1}{k_1 k_2 \cdots k_{\mu'}} \Bigg) \\ &\equiv (-1)^{\mu_0^{(p)}(\mathfrak{G})} \Bigg(\sum_{\substack{\lambda_1,\ldots,\lambda_{\mu_0^{(p)}(\mathfrak{G})} \ge 0 \\ \lambda_1 + \cdots + \lambda_{\mu_0^{(p)}(\mathfrak{G})} = \mu'}} \prod_{j=1}^{\mu_0^{(p)}(\mathfrak{G})} \sum_{\substack{1 \le \kappa_1,\ldots,\kappa_{\lambda_j} \le p-1 \\ \kappa_1 < \cdots < \kappa_{\lambda_j}}} \frac{1}{\kappa_1 \kappa_2 \cdots \kappa_{\lambda_j}} \Bigg) \mod p. \end{aligned} \tag{18}$$

At this stage of the proof, symmetric functions naturally enter the scene, when we observe that modulo p

$$\sum_{\substack{1 \le \kappa_1,\ldots,\kappa_{\lambda_j} \le p-1 \\ \kappa_1 < \cdots < \kappa_{\lambda_j}}} \frac{1}{\kappa_1 \kappa_2 \cdots \kappa_{\lambda_j}} \equiv \sum_{\substack{1 \le \kappa_1,\ldots,\kappa_{\lambda_j} \le p-1 \\ \kappa_1 < \cdots < \kappa_{\lambda_j}}} \kappa_1 \kappa_2 \cdots \kappa_{\lambda_j} = \sigma_{\lambda_j}(1,2,\ldots,p-1) \tag{19}$$

is a value of the elementary symmetric function $\sigma_{\lambda_j}(x_1,\ldots,x_{p-1})$. Indeed, by inverting and reducing a tuple $(\kappa_1,\ldots,\kappa_{\lambda_j})$ modulo p, and then re-ordering the resulting numbers, we obtain an involution on the index set

$$\Big\{ (\kappa_1,\ldots,\kappa_{\lambda_j}) \in [p-1]^{\lambda_j} : \; \kappa_1 < \cdots < \kappa_{\lambda_j} \Big\},$$

identifying terms of the first sum in (19) with congruent terms of the second sum. It is this connection (19) with the theory of symmetric functions, which allows us to considerably simplify the last expression in (18). By the definition of elementary symmetric functions and Fermat's Theorem, we have

$$\sum_{0 \le \nu < p} (-1)^{p-\nu-1} \sigma_{p-\nu-1}(1,2,\ldots,p-1)\, x^\nu = \prod_{0<i<p} (x-i) \equiv x^{p-1} - 1 \mod p,$$

[9]For a positive integer n, we denote by $[n]$ the standard set $\{1,2,\ldots,n\}$ of size n.

which, by comparing coefficients, yields

$$\sigma_j(1,2,\dots,p-1) \equiv \begin{cases} 1, & j=0 \\ -1, & j=p-1 \\ 0, & \text{otherwise} \end{cases} \mod p, \quad j \geq 0. \tag{20}$$

Combining (18) with (19) and (20), it follows that modulo p

$$\begin{aligned} m_{\mathfrak{G}}^{-\mu}\vartheta_\mu(\mathfrak{G}) &\equiv (-1)^{\mu_0^{(p)}(\mathfrak{G})} \sum_{\substack{\lambda_1,\dots,\lambda_{\mu_0^{(p)}(\mathfrak{G})}\in\{0,p-1\} \\ \lambda_1+\cdots+\lambda_{\mu_0^{(p)}(\mathfrak{G})}=\mu'}} \prod_{j=1}^{\mu_0^{(p)}(\mathfrak{G})} \sigma_{\lambda_j}(1,2,\dots,p-1) \\ &\equiv (-1)^{\mu_0^{(p)}(\mathfrak{G})+\mu'/(p-1)} \binom{\mu_0^{(p)}(\mathfrak{G})}{\mu'/(p-1)} \\ &= (-1)^{\frac{\mu(\mathfrak{G})-2\mu_p(\mathfrak{G})+\mu}{p-1}} \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\frac{\mu-\mu_p(\mathfrak{G})}{p-1}}, \end{aligned}$$

and the proof of Lemma 1 is complete. □

4. A partition lemma

By a partition π we mean any sequence $\pi = \{\pi_j\}_{j\geq 1}$ of non-negative integers, such that $\pi_j = 0$ for all but finitely many j. The integer $|\pi| = \sum_{j\geq 1} j\,\pi_j$ is called the *weight* of π, and $||\pi|| = \sum_{j\geq 1}\pi_j$ 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 $\pi \vdash n$ for $|\pi| = n$, and say that π is a partition of n. Moreover, for a positive integer n and a prime p, we denote by $\nu_p(n)$ the p-adic valuation of n, that is, the exponent of p in the prime decomposition of n. We shall require the following observation concerning the product of parts of a partition.

Lemma 2. *Let $\pi = \{\pi_j\}_{j\geq 1}$ be a partition, and let p be a prime. Then we have*

$$\nu_p\Big(\prod_{j\geq 1} j^{\pi_j}\Big) \leq \nu_p\big((p(|\pi| - ||\pi||))!\big) \tag{21}$$

with equality occurring if and only if either $|\pi| = ||\pi||$, or $|\pi| = ||\pi|| + 1$ and $p = 2$.

Proof. For a partition π, denote by $L(\pi)$ the left-hand side of inequality (21), and by $R(\pi)$ the corresponding right-hand side. We establish our claim by induction on the complexity measure $\sum_{j\geq 3}\pi_j$. If $\sum_{j\geq 3}\pi_j = 0$, then

$$L(\pi) = \nu_p(2^{\pi_2}) = \begin{cases} \pi_2, & p = 2 \\ 0, & p \geq 3 \end{cases},$$

while

$$R(\pi) = \nu_p\big((p\pi_2)!\big) \geq \pi_2 + \left\lfloor \frac{\pi_2}{p} \right\rfloor;$$

that is, $L(\pi) \le R(\pi)$ with equality occurring precisely in the cases mentioned. Now let π be a partition with $\sum_{j\ge 3}\pi_j > 0$, and let $j \ge 3$ be some index with $\pi_j \ge 1$. We assume that our claim holds for partitions with smaller complexity. Denote by π' the partition with

$$\pi'_i = \begin{cases} \pi_i, & i \ne j \\ \pi_j - 1, & i = j \end{cases}, \quad i \ge 1.$$

Now

$$L(\pi) = L(\pi') \,+\, \nu_p(j)$$

and, putting $m := |\pi| - ||\pi||$,

$$\begin{aligned} R(\pi) &= R(\pi') \,+\, \nu_p\big((pm)!\big) \,-\, \nu_p\big((p(m-j+1))!\big) \\ &\ge R(\pi') \,+\, j - 1. \end{aligned}$$

Our claim follows now from the inequality $L(\pi') \le R(\pi')$ coming from the induction hypothesis, and the inequality $j < p^{j-1}$, which holds for $p \ge 2$ and all $j \ge 3$. □

5. A functional equation for $X^*_{\mathfrak{G}}(z)$

Fix a prime p, and let $\bar f^{(p)}_\lambda(\mathfrak{G})$ denote the function $f_\lambda(\mathfrak{G})$ evaluated modulo p. The purpose of this section is to establish a functional equation for the generating function

$$X^{*p}_{\mathfrak{G}}(z) = \sum_{\lambda\ge 1} \bar f^{(p)}_\lambda(\mathfrak{G})\, z^\lambda \in GF(p)[[z]]$$

in the case where $m_{\mathfrak{G}}$ is divisible by p. Rewrite (6) in the form

$$f_{\lambda+1}(\mathfrak{G}) = \sum_{\mu=1}^{\mu(\mathfrak{G})} C_\mu^{-1} \sum_{\substack{\lambda_1,\dots,\lambda_\mu>0 \\ \lambda_1+\cdots+\lambda_\mu=\lambda}} p^{-(\nu_p(\mu!)+\mu\nu_p(m_{\mathfrak{G}}))}\, \mathcal{F}^{(\mathfrak{G})}_\mu(\lambda_1,\dots,\lambda_\mu) \prod_{j=1}^{\mu} f_{\lambda_j}(\mathfrak{G}), \quad \lambda \ge 1, \tag{22}$$

with

$$C_\mu := \frac{\mu!}{p^{\nu_p(\mu!)}}\Big(\frac{m_{\mathfrak{G}}}{p^{\nu_p(m_{\mathfrak{G}})}}\Big)^\mu,$$

and decompose $\mathcal{F}^{(\mathfrak{G})}_\mu(\lambda_1,\dots,\lambda_\mu)$ as

$$\mathcal{F}^{(\mathfrak{G})}_\mu(\lambda_1,\dots,\lambda_\mu) = \mu!\,\vartheta_\mu(\mathfrak{G}) \,+\, \Delta^{(\mathfrak{G})}_\mu(\lambda) \,+\, R^{(\mathfrak{G})}_\mu(\lambda_1,\dots,\lambda_\mu),$$

where

$$\Delta^{(\mathfrak{G})}_\mu(\lambda) := \begin{cases} (\mu+1)!\,(\lambda-\mu)\,\vartheta_{\mu+1}(\mathfrak{G})/2, & \mu < \mu(\mathfrak{G}) \\ 0, & \mu = \mu(\mathfrak{G}) \end{cases}$$

and

$$R^{(\mathfrak{G})}_\mu(\lambda_1,\dots,\lambda_\mu) := \sum_{\nu=\mu+2}^{\mu(\mathfrak{G})} \sum_{\substack{\nu_1,\dots,\nu_\mu\ge 0 \\ \nu_1+\cdots+\nu_\mu=\nu-\mu}} \vartheta_\nu(\mathfrak{G})\, \frac{\nu!}{(\nu_1+1)\cdots(\nu_\mu+1)} \binom{\lambda_1-1}{\nu_1}\cdots\binom{\lambda_\mu-1}{\nu_\mu}.$$

By Lemma 1(i) and Lemma 2, we have for $\nu \geq \mu \geq 1$

$$\nu_p\Big(\frac{\nu!\,\vartheta_\nu(\mathfrak{G})}{(\nu_1+1)\cdots(\nu_\mu+1)}\Big) \;\geq\; \nu_p(\nu!) \,+\, \nu\,\nu_p(m_{\mathfrak{G}}) \,-\, \nu_p((p(\nu-\mu))!)$$

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

$$\begin{aligned}\nu_p\Big(\frac{p^{-(\nu_p(\mu!)+\mu\nu_p(m_{\mathfrak{G}}))}\nu!\,\vartheta_\nu(\mathfrak{G})}{(\nu_1+1)\cdots(\nu_\mu+1)}\Big) \;&> \nu_p(\nu!) + \nu\nu_p(m_{\mathfrak{G}}) - \nu_p((p(\nu-\mu))!) - \nu_p(\mu!) - \mu\nu_p(m_{\mathfrak{G}})\\ &\geq \nu - \mu + \nu_p(\nu!) - \nu_p(\mu!) - \nu_p((p(\nu-\mu))!)\\ &= \nu_p\Big(\binom{p\nu}{p\mu}\Big) \geq 0.\end{aligned}$$

Hence, for each $\mu \in [\mu(\mathfrak{G})]$, the term $R_\mu^{(\mathfrak{G})}(\lambda_1,\ldots,\lambda_\mu)$ is divisible by $p^{\nu_p(\mu!)+\mu\nu_p(m_{\mathfrak{G}})}$, and the quotient

$$R_\mu^{(\mathfrak{G})}(\lambda_1,\ldots,\lambda_\mu)/p^{\nu_p(\mu!)+\mu\nu_p(m_{\mathfrak{G}})}$$

is divisible by p. Furthermore, we claim that $\Delta_\mu^{(\mathfrak{G})}(\lambda)$ is also divisible by $p^{\nu_p(\mu!)+\mu\nu_p(m_{\mathfrak{G}})}$ for all $\mu \in [\mu(\mathfrak{G})]$, and that, modulo p,

$$\Delta_\mu^{(\mathfrak{G})}(\lambda)/p^{\nu_p(\mu!)+\mu\nu_p(m_{\mathfrak{G}})} \equiv \begin{cases}\binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1}\,\lambda, & p=2, 2 \mid \mu < \mu(\mathfrak{G}), \nu_2(m_{\mathfrak{G}})=1,\\ & \;\&\; (\zeta_{m_{\mathfrak{G}}/2}(\mathfrak{G}),\zeta_{m_{\mathfrak{G}}}(\mathfrak{G})) \not\equiv (0,1)\,(2)\,.\\ 0, & \text{otherwise}\end{cases} \tag{23}$$

By definition of $\Delta_\mu^{(\mathfrak{G})}(\lambda)$, this is certainly true if $\mu = \mu(\mathfrak{G})$, and also holds for $\mu < \mu(\mathfrak{G})$ and $p \neq 2$ by Lemma 1 (i). Hence, we may suppose that $p = 2$ and that $\mu < \mu(\mathfrak{G})$, and consider divisibility of $(\mu+1)!\vartheta_{\mu+1}(\mathfrak{G})$ by $2^{1+\nu_2(\mu!)+\mu\nu_2(m_{\mathfrak{G}})}$. Now, if μ is odd, then $\nu_2((\mu+1)!) > \nu_2(\mu!)$, and our claim follows from the facts that $m_{\mathfrak{G}} \equiv 0\,(2)$, and that, by Lemma 1 (i), $\vartheta_{\mu+1}(\mathfrak{G})$ is divisible by $2^{(\mu+1)\nu_2(m_{\mathfrak{G}})}$. If, on the other hand, μ is even, then $\nu_2((\mu+1)!) = \nu_2(\mu!)$, and Lemma 1 tells us that $(\mu+1)!\vartheta_{\mu+1}(\mathfrak{G})$ is divisible by $2^{1+\nu_2(\mu!)+\mu\nu_2(m_{\mathfrak{G}})}$, and that

$$(\mu+1)!\,\vartheta_{\mu+1}(\mathfrak{G})/2^{1+\nu_2(\mu!)+\mu\nu_2(m_{\mathfrak{G}})} \equiv 2^{\nu_2(m_{\mathfrak{G}})-1}\binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1} \mod 2. \tag{24}$$

If $\nu_2(m_{\mathfrak{G}}) > 1$, then the right-hand side of (24) vanishes modulo 2. Similarly, if $\nu_2(m_{\mathfrak{G}}) = 1$ and $(\zeta_{m_{\mathfrak{G}}/2}(\mathfrak{G}),\zeta_{m_{\mathfrak{G}}}(\mathfrak{G})) \equiv (0,1)\,(2)$, then

$$\mu(\mathfrak{G}) - \mu_2(\mathfrak{G}) \equiv \zeta_{m_{\mathfrak{G}}/2}(\mathfrak{G}) \equiv 0 \mod 2,$$

while

$$\mu - \mu_2(\mathfrak{G}) + 1 \equiv \zeta_{m_{\mathfrak{G}}}(\mathfrak{G}) \equiv 1 \mod 2,$$

and hence

$$\binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1} \equiv 0 \mod 2.$$

However, if $\nu_2(m_{\mathfrak{G}}) = 1$ and $(\zeta_{m_{\mathfrak{G}}/2}(\mathfrak{G}),\zeta_{m_{\mathfrak{G}}}(\mathfrak{G})) \not\equiv (0,1)\,(2)$, then we can only say that $\Delta_\mu^{(\mathfrak{G})}(\lambda)$ is divisible by $2^{\nu_2(\mu!)+\mu\nu_2(m_{\mathfrak{G}})}$, and that

$$\Delta_\mu^{(\mathfrak{G})}(\lambda)/2^{\nu_2(\mu!)+\mu\nu_2(m_{\mathfrak{G}})} \equiv \binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1}\lambda \mod 2.$$

Our claim (23) is thus proved. Finally, again by the first part of Lemma 1, $\mu!\vartheta_\mu(\mathfrak{G})$ is divisible by $p^{\nu_p(\mu!)+\mu\nu_p(m_\mathfrak{G})}$ for every $\mu \in [\mu(\mathfrak{G})]$, and

$$\mu!\vartheta_\mu(\mathfrak{G})/p^{\nu_p(\mu!)+\mu\nu_p(m_\mathfrak{G})} \equiv (-1)^{\frac{\mu(\mathfrak{G})-2\mu_p(\mathfrak{G})+\mu}{p-1}} C_\mu \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\frac{\mu-\mu_p(\mathfrak{G})}{p-1}} \mod p.$$

Summarizing the previous discussion, we conclude that $\mathcal{F}_\mu^{(\mathfrak{G})}(\lambda_1,\dots,\lambda_\mu)$ is divisible by $p^{\nu_p(\mu!)+\mu\nu_p(m_\mathfrak{G})}$, and that

$$\mathcal{F}_\mu^{(\mathfrak{G})}(\lambda_1\dots,\lambda_\mu)/p^{\nu_p(\mu!)+\mu\nu_p(m_\mathfrak{G})} \equiv (-1)^{\frac{\mu(\mathfrak{G})-2\mu_p(\mathfrak{G})+\mu}{p-1}} C_\mu \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\frac{\mu-\mu_p(\mathfrak{G})}{p-1}} +$$

$$\delta_{p,2}\,\delta_{\nu_2(m_\mathfrak{G}),1}\,(1+\mu)\,\lambda\,(1+\delta_{\mu,\mu(\mathfrak{G})})\,(1+\delta_{\overline{(\zeta_{m_\mathfrak{G}/2}(\mathfrak{G}),\zeta_{m_\mathfrak{G}}(\mathfrak{G}))},(0,1)})\binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1} \mod p, \tag{25}$$

where an overstroke denotes reduction modulo 2. Evaluating (22) modulo p in the light of (25), and noting the fact that

$$f_1(\mathfrak{G}) = \vartheta_0(\mathfrak{G}) = \prod_{\kappa|m_\mathfrak{G}} \prod_{\substack{1\le k\le m_\mathfrak{G}\\(m_\mathfrak{G},k)=\kappa}} k^{\zeta'_\kappa(\mathfrak{G})} \equiv (-1)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}\,\delta_{\mu_p(\mathfrak{G}),0} \mod p,$$

we find for the function $\bar{f}_\lambda^{(p)}(\mathfrak{G})$ the GF(p)-recurrence relation

$$\bar{f}_{\lambda+1}^{(p)}(\mathfrak{G}) = \sum_{\mu=1}^{\mu(\mathfrak{G})} \sum_{\substack{\lambda_1,\dots,\lambda_\mu>0\\ \lambda_1+\dots+\lambda_\mu=\lambda}} \Bigg[(-1)^{\frac{\mu(\mathfrak{G})-2\mu_p(\mathfrak{G})+\mu}{p-1}} \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\frac{\mu-\mu_p(\mathfrak{G})}{p-1}} + \delta_{p,2}\,\delta_{\nu_2(m_\mathfrak{G}),1}\,(1+\mu)\,C_\mu^{-1}\,\lambda$$

$$\times\ (1+\delta_{\mu,\mu(\mathfrak{G})})(1+\delta_{\overline{(\zeta_{m_\mathfrak{G}/2}(\mathfrak{G}),\zeta_{m_\mathfrak{G}}(\mathfrak{G}))},(0,1)})\binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1}\Bigg]\,\bar{f}_{\lambda_1}^{(p)}(\mathfrak{G})\cdots\bar{f}_{\lambda_\mu}^{(p)}(\mathfrak{G})$$

$$\big(\lambda\ge 1,\ \bar{f}_1^{(p)}(\mathfrak{G}) = (-1)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}\delta_{\mu_p(\mathfrak{G}),0}\big). \tag{26}$$

Multiplying both sides of (26) by z^λ and summing over $\lambda \ge 1$, the left-hand side becomes

$$\sum_{\lambda\ge1} \bar{f}_{\lambda+1}^{(p)}(\mathfrak{G})\,z^\lambda = z^{-1}\Big[X_\mathfrak{G}^{*p}(z) - (-1)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}\,\delta_{\mu_p(\mathfrak{G}),0}\,z\Big],$$

while the corresponding right-hand side is the sum of

$$\Sigma_1 := \sum_{\lambda\ge1}\sum_{\mu=1}^{\mu(\mathfrak{G})} \sum_{\substack{\lambda_1,\dots,\lambda_\mu>0\\ \lambda_1+\dots+\lambda_\mu=\lambda}} (-1)^{\frac{\mu(\mathfrak{G})-2\mu_p(\mathfrak{G})+\mu}{p-1}} \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\frac{\mu-\mu_p(\mathfrak{G})}{p-1}} \bar{f}_{\lambda_1}^{(p)}(\mathfrak{G})\cdots\bar{f}_{\lambda_\mu}^{(p)}(\mathfrak{G})\,z^\lambda$$

and

$$\delta_{\nu_2(m_\mathfrak{G}),1}\,\big(1+\delta_{\overline{(\zeta_{m_\mathfrak{G}/2}(\mathfrak{G}),\zeta_{m_\mathfrak{G}}(\mathfrak{G}))},(0,1)}\big)\,\Sigma_2,$$

where

$$\Sigma_2 := \delta_{p,2} \sum_{\lambda\geq 1} \sum_{\mu=1}^{\mu(\mathfrak{G})} \sum_{\substack{\lambda_1,\ldots,\lambda_\mu>0 \\ \lambda_1+\cdots+\lambda_\mu=\lambda}} (1+\mu)\, C_\mu^{-1}\, \lambda\, (1+\delta_{\mu,\mu(\mathfrak{G})}) \binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1} \bar{f}_{\lambda_1}^{(p)}(\mathfrak{G}) \cdots \bar{f}_{\lambda_\mu}^{(p)}(\mathfrak{G})\, z^\lambda.$$

By the binomial law in the ring $\mathrm{GF}(p)[[z]]$,

$$\Sigma_1 = (-1)^{1+\frac{\mu(\mathfrak{G})}{p-1}}\, \delta_{\mu_p(\mathfrak{G}),0} \;+\; \big(X_{\mathfrak{G}}^{*p}(z)\big)^{\mu_p(\mathfrak{G})} \Big(\big(X_{\mathfrak{G}}^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}.$$

Also,

$$\Sigma_2 = \delta_{p,2}\, z \sum_{0<\mu<\mu(\mathfrak{G})} (1+\mu)\, C_\mu^{-1} \binom{\mu(\mathfrak{G})-\mu_2(\mathfrak{G})}{\mu-\mu_2(\mathfrak{G})+1} \Big[\big(X_{\mathfrak{G}}^{*p}(z)\big)^{\mu}\Big]' = 0.$$

The discussion of this section has led to the following result.

Proposition 2. *Let $\mathfrak{G}$ be a finitely generated virtually free group, and let p be a prime dividing $m_{\mathfrak{G}}$. Then the generating function $X_{\mathfrak{G}}^{*p}(z)$ satisfies the identity*

$$X_{\mathfrak{G}}^{*p}(z) = z\big(X_{\mathfrak{G}}^{*p}(z)\big)^{\mu_p(\mathfrak{G})} \Big(\big(X_{\mathfrak{G}}^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}. \tag{27}$$

Equivalently, the function $\bar{f}_\lambda^{(p)}(\mathfrak{G})$ satisfies the GF(p)-recursion

$$\bar{f}_{\lambda+1}^{(p)}(\mathfrak{G}) = \sum_{\nu\geq 0} \sum_{\substack{\pi\vdash\lambda \\ ||\pi||=\nu(p-1)+\mu_p(\mathfrak{G})}} (-1)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}-\nu} \binom{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}{\nu} \times \frac{\big(\nu(p-1)+\mu_p(\mathfrak{G})\big)!}{\prod_{j\geq 1}\pi_j!} \prod_{j\geq 1} \big(\bar{f}_j^{(p)}(\mathfrak{G})\big)^{\pi_j}, \quad \lambda\geq 1, \tag{28}$$

starting from $\bar{f}_1^{(p)}(\mathfrak{G}) = (-1)^{\frac{\mu(\mathfrak{G})-\mu_p(\mathfrak{G})}{p-1}}\, \delta_{\mu_p(\mathfrak{G}),0}$.

6. Free p-patterns: classification, divisibility, and rationality of $X_{\mathfrak{G}}^{*p}(z)$

Given a prime p and a finitely generated virtually free group $\mathfrak{G}$, define the *free p-pattern* $\Pi^{*p}(\mathfrak{G})$ of $\mathfrak{G}$ to be the family

$$\Pi^{*p}(\mathfrak{G}) = \Big\{\Pi_1^{*p}(\mathfrak{G}), \Pi_2^{*p}(\mathfrak{G}), \ldots, \Pi_{p-1}^{*p}(\mathfrak{G})\Big\},$$

where

$$\Pi_i^{*p}(\mathfrak{G}) := \big\{\lambda\in\mathbb{N}:\ f_\lambda(\mathfrak{G}) \equiv i \bmod p\big\}, \quad 0<i<p;$$

in particular, $\Pi_{\mathfrak{G}}^* := \Pi_1^{*2}(\mathfrak{G})$ is called the *free parity pattern* of $\mathfrak{G}$. In this and the following section, we shall exploit identity (27) to obtain results concerning the p-patterns $\Pi^{*p}(\mathfrak{G})$, in the case where $p \mid m_{\mathfrak{G}}$. Our first observation is that $X_{\mathfrak{G}}^{*p}(z) = 0$ is a solution of the functional equation (27) if and only if $\mu_p(\mathfrak{G}) > 0$; that is, we have

$$\mathcal{N}^{*p}(\mathfrak{G}) = \bigcup_{0<i<p} \Pi_i^{*p}(\mathfrak{G}) = \emptyset \Longleftrightarrow \mu_p(\mathfrak{G}) > 0. \tag{29}$$

Hence, we can (and will) from now on restrict attention to the case where $\mu_p(\mathfrak{G}) = 0$. For a prime p, denote by $\mathfrak{V}_p$ the class of all finitely generated virtually free groups $\mathfrak{G}$ satisfying $\mu_p(\mathfrak{G}) = 0$. The groups $\mathfrak{G}_{p,q} = C_p * C_q$ with $q \in \mathbb{N}$ are members of $\mathfrak{V}_p$; in particular, Hecke groups $\mathfrak{H}(q) = \mathfrak{G}_{2,q}$ with $q \geq 3$ are contained in $\mathfrak{V}_2$, as is, for instance, the group $\mathfrak{G} = C_2 * C_2 * C_4$. On the other hand, $\widetilde{\mathfrak{H}}(q) = C_q * C_q$ ($q \geq 3$), which is embedded as a subgroup of index 2 in $\mathfrak{H}(q)$, is never contained in $\mathfrak{V}_2$; in particular, no analogue of the descent principle [24, Theorem 1] holds in the context of free subgroup patterns. For $\mathfrak{G} \in \mathfrak{V}_p$, identity (27) simplifies to

$$X_{\mathfrak{G}}^{*p}(z) = z\Big(\big(X_{\mathfrak{G}}^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G})}{p-1}}, \tag{30}$$

and the recurrence relation (28) takes the form

$$\bar{f}_{\lambda+1}^{(p)}(\mathfrak{G}) = \sum_{\nu \geq 0} \sum_{\substack{\pi \vdash \lambda \\ ||\pi|| = \nu(p-1)}} (-1)^{\frac{\mu(\mathfrak{G})}{p-1} - \nu} \binom{\frac{\mu(\mathfrak{G})}{p-1}}{\nu} \frac{\big(\nu(p-1)\big)!}{\prod_{j \geq 1} \pi_j!} \prod_{j \geq 1} \big(\bar{f}_j^{(p)}(\mathfrak{G})\big)^{\pi_j},$$

$$\big(\lambda \geq 1,\ \bar{f}_1^{(p)}(\mathfrak{G}) = (-1)^{\frac{\mu(\mathfrak{G})}{p-1}}\big); \tag{31}$$

in particular,

$$1 \in \begin{cases} \Pi_1^{(p)}(\mathfrak{G}), & \frac{\mu(\mathfrak{G})}{p-1} \equiv 0\,(2) \\ \Pi_{p-1}^{(p)}(\mathfrak{G}), & \frac{\mu(\mathfrak{G})}{p-1} \equiv 1\,(2). \end{cases}$$

Equation (31) tells us among other things that, for $\mathfrak{G} \in \mathfrak{V}_p$, $\Pi^{*p}(\mathfrak{G})$ is already determined by the free rank $\mu(\mathfrak{G})$, and the question arises whether, conversely, the p-pattern $\Pi^{*p}(\mathfrak{G})$ also determines $\mu(\mathfrak{G})$, or whether there exist virtually free groups having different free ranks while exhibiting the same free p-pattern and having p-rank equal to zero. Our first result shows that the latter situation cannot arise.

Theorem 1. *Let p be a prime, and let $\mathfrak{G}_1, \mathfrak{G}_2 \in \mathfrak{V}_p$. Then we have $\Pi^{*p}(\mathfrak{G}_1) = \Pi^{*p}(\mathfrak{G}_2)$ if and only if $\mu(\mathfrak{G}_1) = \mu(\mathfrak{G}_2)$.*

Proof. We observed already that $\mu(\mathfrak{G}_1) = \mu(\mathfrak{G}_2)$ implies $\Pi^{*p}(\mathfrak{G}_1) = \Pi^{*p}(\mathfrak{G}_2)$. Conversely, let $\mathfrak{G}_1, \mathfrak{G}_2$ be virtually free groups with $\mu_p(\mathfrak{G}_1) = \mu_p(\mathfrak{G}_2) = 0$ and $\Pi^{*p}(\mathfrak{G}_1) = \Pi^{*p}(\mathfrak{G}_2)$. Then $X_{\mathfrak{G}_1}^{*p}(z) = X_{\mathfrak{G}_2}^{*p}(z) =: X^{*p}(z)$, and (30) implies that

$$\Big(\big(X^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G}_1)}{p-1}} = \Big(\big(X^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G}_2)}{p-1}}.$$

Suppose without loss of generality that $\mu(\mathfrak{G}_1) \leq \mu(\mathfrak{G}_2)$, and rewrite the last equation as

$$\Big(\big(X^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G}_1)}{p-1}} \Big[\Big(\big(X^{*p}(z)\big)^{p-1} - 1\Big)^{\vartheta} - 1\Big] = 0,$$

where

$$\vartheta := \frac{\mu(\mathfrak{G}_2) - \mu(\mathfrak{G}_1)}{p-1} \geq 0.$$

Since $\bar{f}_1^{(p)}(\mathfrak{G}) \neq 0$ and $GF(p)[[z]]$ has no zero divisors, we obtain the $GF(p)$-relation

$$1 = \Big(\big(X^{*p}(z)\big)^{p-1} - 1\Big)^{\vartheta} = \sum_{\nu=0}^{\vartheta} (-1)^{\vartheta-\nu} \binom{\vartheta}{\nu} \big(X^{*p}(z)\big)^{(p-1)\nu}.$$

Again using the fact that $\bar{f}_1^{(p)}(\mathfrak{G}) \neq 0$ and comparing coefficients, we now deduce that $\binom{\vartheta}{\nu} \equiv 0\,(p)$ for all $\nu \in [\vartheta]$, which is impossible for $\vartheta > 0$. Hence, we must have $\mu(\mathfrak{G}_1) = \mu(\mathfrak{G}_2)$. □

Our next result determines those groups $\mathfrak{G} \in \mathfrak{V}_p$ for which the series $X_{\mathfrak{G}}^{*p}(z)$ is a rational function.

Theorem 2. *Let p be a prime, and let $\mathfrak{G} \in \mathfrak{V}_p$. Then the following assertions are equivalent:*

(i) *$X_{\mathfrak{G}}^{*p}(z)$ is rational over $GF(p)$,*

(ii) *$\mu(\mathfrak{G}) = 0$, or $\mu(\mathfrak{G}) = 1$ and $p = 2$,*

(iii) *$\mathfrak{G}$ is finite of order divisible by p, or $\mathfrak{G} \cong G_1 *_S G_2$ with finite groups G_i, S of odd order, $(G_1 : S) = (G_2 : S) = 2$, and $p = 2$.*

Proof. If $\mu(\mathfrak{G}) = \mu_p(\mathfrak{G}) = 0$, that is, $\mathfrak{G}$ finite of order divisible by p, then $X_{\mathfrak{G}}^{*p}(z) = z$. Moreover, for $\mu_p(\mathfrak{G}) = 0$, $\mu(\mathfrak{G}) = 1$, and $p = 2$, the series $X_{\mathfrak{G}}^{*p}(z) = \frac{z}{1-z}$ is a solution of (27). Thus, (ii) implies (i). To prove the converse, suppose first that $\mu_p(\mathfrak{G}) = 0$ and $\mu(\mathfrak{G}) \geq 2$, let $X_{\mathfrak{G}}^{*p}(z) = \varphi^*(z)/\psi^*(z)$ with relatively prime polynomials $\varphi^*(z), \psi^*(z) \in GF(p)[z]$, and let $v = \deg(\varphi^*(z)) - \deg(\psi^*(z))$ be the (total) degree of $X_{\mathfrak{G}}^{*p}(z)$. Multiplying both sides by $(\psi^*(z))^{\mu(\mathfrak{G})}$, equation (30) takes the form

$$\varphi^*(z)\big(\psi^*(z)\big)^{\mu(\mathfrak{G})-1} = z\Big[\big(\varphi^*(z)\big)^{p-1} - \big(\psi^*(z)\big)^{p-1}\Big]^{\frac{\mu(\mathfrak{G})}{p-1}}. \tag{32}$$

Since $\mu(\mathfrak{G}) \geq 2$, $\psi^*(z)$ must divide the right-hand side of (32), as it divides the left-hand side, hence $\psi^*(z) \mid z(\varphi^*(z))^{\mu(\mathfrak{G})}$. Thus, as $(\varphi^*(z), \psi^*(z)) = 1$, it follows that $\psi^*(z) \mid z$, and hence that $\psi^*(z) \in GF(p)\backslash\{0\}$, since $\psi^*(z)$ must have a non-zero constant term; in particular, $v = \deg(\varphi^*(z)) \geq 0$. Comparing degrees on both sides of (30) now gives

$$(\mu(\mathfrak{G}) - 1)v + 1 = 0,$$

which is impossible for $v \geq 0$. This contradiction establishes the implication (i) ⇒ (ii) in the case where $\mu(\mathfrak{G}) \geq 2$. The equivalence of (ii) and (iii) under the assumption $\mu_p(\mathfrak{G}) = 0$, as well as the fact that for $p > 2$ and $\mu(\mathfrak{G}) = 1$ we have $\mu_p(\mathfrak{G}) > 0$, follow from the well-known classification of virtually infinite-cyclic groups (that is, finitely generated groups with two ends); cf. for instance [32, Sect. 5.1], [36, Lemma 4.1], or the remark preceding [16, Corollary 6]. □

Corollary 1. *If $\mathfrak{G} \in \mathfrak{V}_p$ and $\mu(\mathfrak{G}) \geq 1$, then the set $\mathcal{N}^{*p}(\mathfrak{G})$ is infinite.*

The following result describes a divisibility property of the set $\mathcal{N}^{*p}(\mathfrak{G})$ for $\mathfrak{G} \in \mathfrak{V}_p$. Moreover, we determine the second entry $\alpha_{\mathfrak{G}}^{*p} := \min_{\lambda \in \mathcal{N}^{*p}(\mathfrak{G})\backslash\{1\}} \lambda$ of $\mathcal{N}^{*p}(\mathfrak{G})$, as well as the value of $\bar{f}_{\alpha_{\mathfrak{G}}^{*p}}^{(p)}(\mathfrak{G})$.

Theorem 3. *Let p be a prime, let $\mathfrak{G} \in \mathfrak{V}_p$, and suppose that $\mu(\mathfrak{G}) \geq 1$. Then*

(i) *every entry of $\mathcal{N}^{*p}(\mathfrak{G})$ is congruent to 1 modulo $(p-1)p^{\nu_p(\mu(\mathfrak{G}))}$;*

(ii) *we have $\alpha_{\mathfrak{G}}^{*p} = 1 + (p-1)p^{\nu_p(\mu(\mathfrak{G}))}$ and*

$$\bar{f}^{(p)}_{\alpha_{\mathfrak{G}}^{*p}}(\mathfrak{G}) = (-1)^{\frac{\mu(\mathfrak{G})}{p-1}-1}\left\langle p^{\nu_p(\mu(\mathfrak{G}))} \mid \mu(\mathfrak{G})/(p-1)\right\rangle.$$

Proof. (i) Put $\ell := \nu_p(\mu(\mathfrak{G}))$. We establish the implication

$$\bar{f}^{(p)}_{\lambda+1}(\mathfrak{G}) \neq 0 \Longrightarrow \lambda \equiv 0 \mod (p-1)p^{\ell} \tag{33}$$

for all $\lambda \in \mathbb{N}_0$ by induction on λ. Implication (33) holds trivially if $\lambda = 0$. Suppose that (33) holds for all non-negative integers $\lambda < L$ with some integer $L \geq 1$, and that $\bar{f}^{(p)}_{L+1}(\mathfrak{G}) \neq 0$. By (31) and our inductive hypothesis,

$$\bar{f}^{(p)}_{L+1}(\mathfrak{G}) = \sum_{\substack{\nu \geq 0 \\ \binom{\frac{\mu(\mathfrak{G})}{p-1}}{\nu} \not\equiv 0\,(p)}} \sum_{\substack{\pi \vdash L \\ \pi_j > 0 \Rightarrow j \equiv 1\,((p-1)p^{\ell}) \\ ||\pi|| = \nu(p-1)}} (-1)^{\frac{\mu(\mathfrak{G})}{p-1}-\nu} \binom{\frac{\mu(\mathfrak{G})}{p-1}}{\nu} \frac{\big(\nu(p-1)\big)!}{\prod_{j\geq 1}\pi_j!} \prod_{j\geq 1}\big(\bar{f}^{(p)}_j(\mathfrak{G})\big)^{\pi_j}.$$

If the right-hand side of the latter equation is to be non-zero, then in particular there must exist a pair (ν, π) consisting of a non-negative integer ν such that $\binom{\frac{\mu(\mathfrak{G})}{p-1}}{\nu} \not\equiv 0\,(p)$ and a partition π of weight L and norm $\nu(p-1)$ all of whose parts are congruent to 1 modulo $(p-1)p^{\ell}$. The first and last condition on π imply that

$$L \equiv ||\pi|| \mod (p-1)p^{\ell},$$

while the condition on ν, in view of Lucas' Theorem,[10] forces ν to be divisible by p^{ℓ}. Since $||\pi|| = \nu(p-1)$, we conclude that L is divisible by $(p-1)p^{\ell}$, as claimed.

(ii) Arguing as above by means of Lucas' formula, we see that, for $\lambda = (p-1)p^{\ell}$, the double sum on the right-hand side of (31) contains only one relevant summand, namely the one with $(\nu, \pi) = (p^{\ell}, (1^{(p-1)p^{\ell}}))$. A calculation repeatedly using Fermat's Theorem now yields the value of $\bar{f}^{(p)}_{1+(p-1)p^{\ell}}(\mathfrak{G})$ given in the theorem, and (ii) follows from part (i) and this calculation. □

7. A combinatorial description of $\Pi^{*p}(\mathfrak{G})$

Here, we shall obtain a description of the patterns $\Pi^{*p}(\mathfrak{G})$ for $\mathfrak{G} \in \mathfrak{V}_p$ in terms of the behaviour modulo p of certain parametrized binomial coefficients. Moreover, we derive an explicit characterization of the set

$$\mathcal{N}^{*p}(\mathfrak{G}) = \big\{\lambda \in \mathbb{N} :\ f_{\lambda}(\mathfrak{G}) \not\equiv 0 \bmod p\big\}$$

in terms of Kummer's function $\mathfrak{s}_p$, and we discuss the conditions, under which $\mathcal{N}^{*p}(\mathfrak{G})$ has a description in closed form, in this way obtaining an optimal generalization of Stothers' formula for the parity of $f_{\lambda}(PSL_2(\mathbb{Z}))$; cf. [34]. Use the recurrence relation

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

(31), viewed as an equation over $\mathbb{Z}$, to define an integral sequence $\hat{f}_\lambda^{(p)}(\mathfrak{G})$ starting from $\hat{f}_1^{(p)}(\mathfrak{G}) = (-1)^{\frac{\mu(\mathfrak{G})}{p-1}}$, and let

$$\hat{X}_{\mathfrak{G}}^{*p}(z) := \sum_{\lambda\geq 1} \hat{f}_\lambda^{(p)} z^\lambda \in \mathbb{Z}[[z]].$$

Then we have $\hat{X}_{\mathfrak{G}}^{*p}(z) \equiv X_{\mathfrak{G}}^{*p}(z) \bmod p$, and the series $\hat{X}_{\mathfrak{G}}^{*p}(z)$ satisfies the functional equation

$$\hat{X}_{\mathfrak{G}}^{*p}(z) = z\Big(\big(\hat{X}_{\mathfrak{G}}^{*p}(z)\big)^{p-1} - 1\Big)^{\frac{\mu(\mathfrak{G})}{p-1}}. \tag{34}$$

The latter equation can be rewritten as

$$\hat{X}_{\mathfrak{G}}^{*p}(z) = z\,\Phi\big(\hat{X}_{\mathfrak{G}}^{*p}(z)\big),$$

where

$$\Phi(\zeta) := \big(\zeta^{p-1} - 1\big)^{\frac{\mu(\mathfrak{G})}{p-1}}.$$

By Lagrange inversion, we find that, for $\lambda \geq 1$

$$\Big\langle z^\lambda \mid \hat{X}_{\mathfrak{G}}^{*p}(z)\Big\rangle = \frac{1}{\lambda}\Big\langle \zeta^{\lambda-1} \mid \big(\Phi(\zeta)\big)^\lambda\Big\rangle = (-1)^{\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}}\,\lambda^{-1}\binom{\frac{\mu(\mathfrak{G})\lambda}{p-1}}{\frac{\lambda-1}{p-1}},$$

that is,

$$\hat{X}_{\mathfrak{G}}^{*p}(z) = \sum_{\lambda\geq 1}(-1)^{\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}}\,\lambda^{-1}\binom{\frac{\mu(\mathfrak{G})\lambda}{p-1}}{\frac{\lambda-1}{p-1}} z^\lambda. \tag{35}$$

The first part of our next result follows immediately from (35).

Theorem 4. *Let p be a prime, and let $\mathfrak{G} \in \mathfrak{V}_p$.*

(i) *For $0 < i < p$,*

$$\Pi_i^{*p}(\mathfrak{G}) = \Big\{\lambda \in \mathbb{N} :\ \frac{1}{\lambda}\binom{\frac{\mu(\mathfrak{G})\lambda}{p-1}}{\frac{\lambda-1}{p-1}} \equiv (-1)^{\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}}\, i \bmod p\Big\}.$$

(ii) *We have*

$$\mathcal{N}^{*p}(\mathfrak{G}) = \Big\{\lambda \in \mathbb{N} :\ \mathfrak{s}_p\Big(\frac{\lambda-1}{p-1}\Big) + \mathfrak{s}_p\Big(\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}\Big) - \mathfrak{s}_p\Big(\frac{\mu(\mathfrak{G})\lambda}{p-1}\Big) - \mathfrak{s}_p(\lambda-1) + \mathfrak{s}_p(\lambda) = 1\Big\},$$

where $\mathfrak{s}_p(x)$ denotes the sum of digits in the p-adic expansion of x.

Proof. We only need to consider part (ii). By Kummer's formula[11] for the p-adic norm of binomial coefficients we have

$$(p-1)\,\nu_p\binom{a}{b} = \mathfrak{s}_p(b) + \mathfrak{s}_p(a-b) - \mathfrak{s}_p(a)$$

[11] Cf. [12, pp. 115–116].

with $\mathfrak{s}_p(x)$ as defined in the theorem. Moreover, writing out the p-adic expansions of λ and $\lambda-1$, we find that

$$(p-1)\,\nu_p(\lambda) = \mathfrak{s}_p(\lambda-1) - \mathfrak{s}_p(\lambda) + 1, \quad \lambda \geq 1.$$

Hence,

$$(p-1)\,\nu_p\Big(\frac{1}{\lambda}\left(\begin{smallmatrix}\frac{\mu(\mathfrak{G})\lambda}{p-1}\\ \frac{\lambda-1}{p-1}\end{smallmatrix}\right)\Big) = \mathfrak{s}_p\Big(\frac{\lambda-1}{p-1}\Big) + \mathfrak{s}_p\Big(\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}\Big) - \mathfrak{s}_p\Big(\frac{\mu(\mathfrak{G})\lambda}{p-1}\Big) - \mathfrak{s}_p(\lambda-1) + \mathfrak{s}_p(\lambda) - 1,$$

and (ii) follows from equation (35). □

As is apparent from Theorem 4, neither the patterns $\Pi^{*p}(\mathfrak{G})$ nor the sets $\mathcal{N}^{*p}(\mathfrak{G})$ will in general lend themselves to a characterization in closed form as in the case of the modular group; instead, $\Pi^{*p}(\mathfrak{G})$ and $\mathcal{N}^{*p}(\mathfrak{G})$ generically tend to inherit the well-known kind of fractal behaviour observed in Pascal's triangle when evaluated modulo a prime. There is however one special case where we can describe the sets $\mathcal{N}^{*p}(\mathfrak{G})$ in a completely explicit way, namely when $\mu(\mathfrak{G})$ is a 2-power and $p=2$. For a prime p and a group $\mathfrak{G} \in \mathfrak{V}_p$ with $\mu(\mathfrak{G}) \geq 2$, define

$$\Lambda_{\mathfrak{G}}^{*p} := \left\{ \frac{\big((p-1)\mu(\mathfrak{G})\big)^{\sigma} - 1}{(p-1)\mu(\mathfrak{G}) - 1} : \ \sigma = 1, 2, \dots \right\},$$

that is, $\Lambda_{\mathfrak{G}}^{*p}$ is the set of partial sums of the geometric series $\sum_{\sigma\geq 0}\big((p-1)\mu(\mathfrak{G})\big)^{\sigma}$.

Theorem 5. *Let p be a prime, let $\mathfrak{G} \in \mathfrak{V}_p$, and suppose that $\mu(\mathfrak{G}) \geq 2$. Then the following assertions are equivalent:*

(i) $\mathcal{N}^{*p}(\mathfrak{G}) = \Lambda_{\mathfrak{G}}^{*p}$.

(ii) $\bar{f}_{\lambda}^{(p)}(\mathfrak{G}) = 0$ *for* $2 \leq \lambda \leq (p-1)\mu(\mathfrak{G})$.

(iii) $\mu(\mathfrak{G})$ *is a 2-power, and* $p = 2$.

Proof. Since (i) clearly implies (ii), it suffices to prove the implications (ii) ⇒ (iii) and (iii) ⇒ (i). Suppose first that $\mu(\mathfrak{G})$ is not a p-power, that is, $\mu(\mathfrak{G}) = p^{\ell}m$ with $\ell \geq 0$ and some integer $m > 1$ not divisible by p. Then, by part (ii) of Theorem 3,

$$1 < \alpha_{\mathfrak{G}}^{*p} = 1 + (p-1)p^{\ell} < 1 + (p-1)\mu(\mathfrak{G}),$$

contradicting (ii). Thus, condition (ii) forces $\mu(\mathfrak{G})$ to be a p-power; but then we also must have $p = 2$, since $\mu(\mathfrak{G})$ has to be divisible by $p-1$. This proves the implication (ii) ⇒ (iii). Now suppose that $\mu(\mathfrak{G})$ is a 2-power, say, $\mu(\mathfrak{G}) = 2^{\ell}$ with some $\ell \geq 1$, and

that $p = 2$. Then

$$\begin{aligned}
\mathfrak{s}_p(\lambda) &= \mathfrak{s}_2(\lambda),\\
\mathfrak{s}_p(\lambda-1) &= \mathfrak{s}_2(\lambda-1),\\
\mathfrak{s}_p\Big(\frac{\lambda-1}{p-1}\Big) &= \mathfrak{s}_2(\lambda-1),\\
\mathfrak{s}_p\Big(\frac{\mu(\mathfrak{G})\lambda}{p-1}\Big) &= \mathfrak{s}_2(\lambda),\\
\mathfrak{s}_p\Big(\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}\Big) &= \mathfrak{s}_2((\mu(\mathfrak{G})-1)\lambda+1),
\end{aligned}$$

and the condition on λ in the second part of Theorem 4 simplifies to

$$\mathfrak{s}_2\big((\mu(\mathfrak{G})-1)\lambda+1\big) = 1,$$

or, equivalently,

$$\lambda = \frac{2^\alpha - 1}{2^\ell - 1} \text{ with some } \alpha \geq 1 \text{ such that } \ell \mid \alpha.$$

Assertion (i) with $p = 2$ follows now from Theorem 4 (ii), and the proof of Theorem 5 is complete. □

If $\mathfrak{G} = \mathfrak{H}(q)$ is a Hecke group for some odd $q > 2$, then $\mu(\mathfrak{H}(q)) = q - 1 \geq 2$, and, by specializing Theorem 5 to the case where $p = 2$ and $\mathfrak{G} = \mathfrak{H}(q)$ with a prime $q \geq 3$, we obtain a new characterization of Fermat primes among the set of all odd prime numbers in terms of the free parity pattern of the associated Hecke group.

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

(i) $\Pi^*_{\mathfrak{H}(q)} = \Lambda^{*2}_{\mathfrak{H}(q)} = \left\{ \dfrac{(q-1)^\sigma - 1}{q-2} : \ \sigma = 1, 2, \dots \right\}$.

(ii) $\bar{f}^{(2)}_\lambda(\mathfrak{H}(q)) = 0$ *for* $1 < \lambda < q$.

(iii) *q is a Fermat prime.*

For general $\mathfrak{G} \in \mathfrak{V}_p$, we can at least show that those values λ, such that $f_\lambda(\mathfrak{G})$ is not divisible by p are quite rare. Set

$$N^{*p}_{\mathfrak{G}}(x) = |\{\lambda \leq x : p \nmid f_\lambda(\mathfrak{G})\}|.$$

Corollary 3. *Let p be a prime, and let $\mathfrak{G} \in \mathfrak{V}_p$. Then we have $N^{*p}_{\mathfrak{G}}(x) \ll x^{1-\delta}$ for some $\delta > 0$ depending on p and $\mu(\mathfrak{G})$.*

Proof. It suffices to consider the case $x = p^n, n \in \mathbb{N}$. Let $\alpha \in [0, 1]$ be a parameter to be chosen later. Let $\lambda \leq p^n$ be an element of $\mathcal{N}^{*p}_{\mathfrak{G}}$. Then, by Theorem 4, we either have

$$\mathfrak{s}_p(\lambda - 1) - \mathfrak{s}_p(\lambda) \geq \alpha n \tag{36}$$

or

$$\mathfrak{s}_p\left(\frac{\lambda-1}{p-1}\right) + \mathfrak{s}_p\left(\frac{(\mu(\mathfrak{G})-1)\lambda+1}{p-1}\right) - \mathfrak{s}_p\left(\frac{\mu(\mathfrak{G})}{p-1}\right) \leq \alpha n + 1. \tag{37}$$

An integer λ satisfies (36) if and only if $\nu_p(\lambda) \geq \alpha n + 1$, hence the number of such $\lambda \leq p^n$ is $\ll p^{(1-\alpha)n}$, which is of acceptable size for any $\alpha > 0$. Writing $l = \frac{\lambda-1}{p-1}$, we see that λ satisfies (37) if and only if in the addition

$$l + \big(\mu(\mathfrak{G})l + \mu(G)/(p-1)\big)$$

there are at most $(\alpha n + 1)/(p-1)$ carries. For all but $\mathcal{O}(p^{(1-\alpha/p)n})$ values of l, the term $\mu(\mathfrak{G})/(p-1)$ affects less than $\alpha n/p$ carries, hence, it suffices to consider the addition $l + \mu(\mathfrak{G})l$. Let k be an integer such that $p^k > \mu(\mathfrak{G})$, and write $l = \sum_i l_i p^i$, $l_i \in \{0, 1, \ldots, p-1\}$. A carry occurs at the i-th digit if and only if

$$\left\{\frac{l}{p^i}\right\} + \left\{\frac{\mu(\mathfrak{G})l}{p^i}\right\} \geq 1,$$

where $\{x\}$ denotes the fractional part of x. If $l_{i-1} = \cdots = l_{i-k} = p-1$, a carry necessarily occurs at the i-th digit, since $\{l/p^i\} \geq 1 - p^{-k}$, and

$$\left\{\frac{\mu(\mathfrak{G})l}{p^i}\right\} \geq 1 - \frac{\mu(\mathfrak{G})}{p^k} \geq \frac{1}{p^k}.$$

Thus, if λ satisfies (37), there are at most $m = \frac{2\alpha n}{p-1}$ such strings of consecutive $(p-1)$'s in l. If $\lambda < p^n$, $l < p^n$ as well, and the number of integers $l \leq p^n$ with at most m strings of k consecutive digits $p-1$ is bounded above by

$$\begin{aligned} p^k \binom{\lfloor n/k \rfloor}{m} (p^k - 1)^{\lfloor n/k \rfloor - m} &\ll p^{n-km} \left(\frac{n}{km}\right)^m \left(1 - \frac{1}{p^k}\right)^{\lfloor n/k \rfloor - m} \\ &\ll p^n e^{-n/(kp^k) + 2\alpha n \log \alpha^{-1}} \ll p^{(1-\delta)n}, \end{aligned}$$

provided that α is sufficiently small. From these estimates, our claim follows. □

An Example

If $\mu(\mathfrak{G})$ is not a 2-power, or if $p > 2$, then we are outside the scope of Theorem 5, and cannot hope to be able to describe the p-pattern $\Pi^{*p}(\mathfrak{G})$ or the set $\mathcal{N}^{*p}(\mathfrak{G})$ by means of a closed formula of Stothers' type (or indeed, in any closed form). Nevertheless, Theorem 4 still provides a fairly explicit description of these objects. As an illustration, let $p = 2$, and consider groups $\mathfrak{G} \in \mathfrak{V}_2$ for which $\mu(\mathfrak{G}) - 1$ is a non-trivial 2-power, say, $\mu(\mathfrak{G}) = 2^\rho + 1$ with some $\rho \geq 1$. Then

$$\mathfrak{s}_p\Big(\frac{(\mu(\mathfrak{G}) - 1)\lambda + 1}{p-1}\Big) = \mathfrak{s}_2(2^\rho\lambda + 1) = \mathfrak{s}_2(\lambda) + 1,$$

and the condition on λ in Theorem 4 (ii) becomes

$$2\mathfrak{s}_2(\lambda) = \mathfrak{s}_2(2^\rho\lambda + \lambda).$$

The latter condition holds if and only if the binary representations $\lambda = \sum_{j\geq 0} \lambda_j 2^j$ of λ respectively $2^\rho\lambda = \sum_{j\geq 0} \lambda_j 2^{j+\rho}$ of $2^\rho\lambda$ do not overlap, that is, if and only if $\lambda_j = 1$

always implies $\lambda_{j+\rho} = 0$. Hence, we find from Theorem 4 (ii) that

$$\Pi^*_{\mathfrak{G}} = \left\{ \lambda = \sum_{j\geq 0} \lambda_j 2^j \in \mathbb{N} : \ \lambda_j = 1 \Rightarrow \lambda_{j+\rho} = 0 \ \text{ for all } \ j \geq 0 \right\}$$

$$(\mathfrak{G} \in \mathfrak{V}_2, \mu(\mathfrak{G}) = 2^\rho + 1, \rho \geq 1). \quad (38)$$

This is a rather useful description of $\Pi^*_{\mathfrak{G}}$ for these groups $\mathfrak{G}$; for instance, we immediately infer from (38) that

$$\Pi^*_{\mathfrak{G}} \cap [2^\rho + 1] = [2^\rho].$$

Moreover, in this case we can refine Corollary 3 by giving an asymptotic formula for the number $P^*_G(x)$ of integers $\lambda \leq x$ with $f_\lambda(G) \equiv 1 \pmod 2$.

Proposition 3. *Let $\mathfrak{G} \in \mathfrak{V}_2$ be a group with $\mu(\mathfrak{G}) = 2^\rho + 1$ for some integer ρ. Then there exists a continuous and almost everywhere differentiable function $\tilde{g} : [0, \rho] \to (0, \infty)$, such that*

$$P^*_G(x) \sim \tilde{g}\left(\rho \left\lfloor \frac{\log x}{\rho \log 2} \right\rfloor\right) x^{\frac{\log \varphi}{\log 2}} \quad \text{as } x \to \infty.$$

Here, $\varphi = \frac{1+\sqrt{5}}{2}$.

Proof. First, we consider $P^*_{\mathfrak{G}}(2^{n\rho})$. By (38), this equals the number of ρ-tuples of 01-strings of length n, which do not contain two consecutive digits 1, that is, $P^*_{\mathfrak{G}}(2^{\rho n}) = F^\rho_{n+2}$, where F_m denotes the m-th Fibonacci-number. Here we adopt the convention that $F_1 = F_2 = 1$. Next, consider $P^*_{\mathfrak{G}}(a2^{\rho n})$ for some integer $a \geq 2^\rho$. Denote by α the number of 1's occurring among the last ρ digits of a. Then we have

$$P^*_{\mathfrak{G}}\big((a+1)2^{\rho n} - 1\big) - P^*_{\mathfrak{G}}(a2^{\rho n}) = \begin{cases} 0, & f_a(\mathfrak{G}) \equiv 0 \ (2) \\ F^\alpha_{n+1} F^{\rho-\alpha}_{n+2}, & f_a(\mathfrak{G}) \equiv 1 \ (2). \end{cases}$$

Indeed, if $f_a(\mathfrak{G}) \equiv 0\,(2)$, then there are two 1's in the binary expansion of a with distance ρ, thus the same holds true for all $\lambda \in [a2^{\rho n}, (a+1)2^{\rho n} - 1]$. If on the other hand $f_a(\mathfrak{G}) \equiv 1\,(2)$, then no restriction is imposed on the first digits of such λ, hence, $P^*_{\mathfrak{G}}((a+1)2^{\rho n} - 1) - P^*_{\mathfrak{G}}(a2^{\rho n})$ equals the number of ρ-tuples of 01-strings of length n which do not contain two consecutive 1's, and do not start with 1, whenever the corresponding digit of a among its last ρ digits is 1. For a real number $\eta \in [1, 2^\rho]$, define

$$g(\eta, n) := P^*_{\mathfrak{G}}(\eta 2^{\rho n})\varphi^{-\rho n}.$$

From what we have seen so far, we deduce that the limit

$$g(\eta) := \lim_{n\to\infty} g(\eta, n)$$

exists for all $\eta = \frac{a}{2^k}$, where a is integral and $2^k \leq a \leq 2^{k+\rho}$. Clearly, $g(\eta, n)$ is non-decreasing with η, and, for k fixed and $n \to \infty$, we have

$$g\Big(\frac{a+1}{2^{k\rho}}, n\Big) - g\Big(\frac{a}{2^{k\rho}}, n\Big) = \frac{F^\alpha_{n-k+1} F^{\rho-\alpha}_{n-k+2}}{\varphi^{\rho n}} \ll \varphi^{-k\rho},$$

that is, $g(\eta, n)$ is continuous in η with modulus of continuity $\Phi(g, \delta) \ll \delta^{(\log\varphi)/(\log 2)}$. As $n \to \infty$, $g(\eta, n)$ converges uniformly, hence $g(\eta)$ exists for all $\eta \in [1, 2^\rho]$ and is

continuous with the same modulus of continuity. Putting $\tilde{g}(\eta) = g(2^\eta)\varphi^{-2^\eta}$, we obtain our claim. □

Note that $\tilde{g}$ is highly irregular, for instance, $\tilde{g}(0) = \tilde{g}(\rho)$, while for almost all $\eta \in [0, \rho]$ the function $\tilde{g}(\eta)$ is differentiable in η with $\tilde{g}'(\eta) = -\log(2)\log(\varphi)2^\eta\varphi^{-2^\eta} < 0$. Such behaviour is typical for digital problems, cf. for example [4].

8. Some combinatorial interpretations of the series $\hat{X}^{*2}_{\mathfrak{G}}(z)$

In Section 7 we associated, for each prime p and every group $\mathfrak{G} \in \mathfrak{V}_p$, a canonical lifting $\hat{X}^{*p}_{\mathfrak{G}}(z) \in \mathbb{Z}[[z]]$ to the $GF(p)$-series $X^{*p}_{\mathfrak{G}}(z) = \sum_{\lambda\geq 1} \bar{f}^{(p)}_\lambda(\mathfrak{G})\, z^\lambda$. In this final section, we shall describe a number of combinatorial interpretations for the coefficients of these liftings $\hat{X}^{*p}_{\mathfrak{G}}(z)$ in the case where $p = 2$ and $\mu(\mathfrak{G}) \geq 2$. Let S be a set of positive integers. By a *plane S-tree* we mean a plane tree with the property that every non-terminal vertex has (outer) degree an element of S. Given $S \subseteq \mathbb{N}$ and non-negative integers m, n, we denote by $T_S(m, n)$ the number of plane S-trees having m terminal vertices and a total of n vertices. Let

$$U_S = U_S(t, z) := \sum_{n\geq 0} \sum_{m\geq 0} T_S(m, n)\, t^m\, z^n.$$

Then U_S satisfies the functional equation[12]

$$U_S = tz \,+\, z \sum_{\sigma\in S} U_S^\sigma. \tag{39}$$

In order to establish a connection with the series $\hat{X}^{*2}_{\mathfrak{G}}(z)$, put $S = \{\mu(\mathfrak{G})\}$ and $t = -1/z$. Then equation (39) becomes

$$U_{\{\mu(\mathfrak{G})\}}(-1/z, z) + 1 = z\Big(U_{\{\mu(\mathfrak{G})\}}(-1/z, z)\Big)^{\mu(\mathfrak{G})},$$

and, in view of (34), we must have

$$\hat{X}^{*2}_{\mathfrak{G}}(z) = 1 \,+\, U_{\{\mu(\mathfrak{G})\}}(-1/z, z).$$

Consequently, for $\mathfrak{G} \in \mathfrak{V}_2$, $\mu(\mathfrak{G}) \geq 2$, and $\lambda \geq 1$,

$$\lambda^{-1}\binom{\mu(\mathfrak{G})\lambda}{\lambda - 1} = (-1)^{(\mu(\mathfrak{G})-1)\lambda+1}\big\langle z^\lambda \mid \hat{X}^{*2}_{\mathfrak{G}}(z)\big\rangle = (-1)^{(\mu(\mathfrak{G})-1)\lambda+1}\big\langle z^\lambda \mid U_{\{\mu(\mathfrak{G})\}}(-1/z, z)\big\rangle$$

equals

(a) the number of plane trees with exactly λ non-terminal vertices, each of which having (outer) degree precisely $\mu(\mathfrak{G})$; in particular, $f_\lambda(\mathfrak{G})$ is congruent modulo 2 to the number of these trees.

These tree numbers in turn can be reinterpreted in terms of other combinatorial objects. For $\lambda \geq 1$, $(-1)^{(\mu(\mathfrak{G})-1)\lambda+1}\big\langle z^\lambda \mid \hat{X}^{*2}_{\mathfrak{G}}(z)\big\rangle$ also equals

[12] Cf. [33, Proposition 6.2.4].

(b) the number of sequences $i_1 i_2, \cdots i_{\lambda\mu(\mathfrak{G})}$ with $i_j \in \{-1, \mu(\mathfrak{G}) - 1\}$ for all $j \in [\lambda\mu(\mathfrak{G})]$, such that (i) there are a total of $(\mu(\mathfrak{G}) - 1)\lambda$ values of j for which $i_j = -1$, and (ii) we have $i_1 + i_2 + \cdots + i_j \geq 0$ for all j,

(c) the number of bracketings of a word of length $\lambda(\mu(\mathfrak{G}) - 1) + 1$ subject to λ $\mu(\mathfrak{G})$-ary operations,

(d) the number of paths p in the (x, y)-plane starting in the origin $(0, 0)$ and terminating in the point $(\lambda\mu(\mathfrak{G}), 0)$, using steps $(1, \sigma)$ with $\sigma \in \{-1, \mu(\mathfrak{G}) - 1\}$, such that p never passes below the x-axis,

(e) the number of paths q in the (x, y)-plane from $(0, 0)$ to $((\mu(\mathfrak{G})-1)\lambda, (\mu(\mathfrak{G})-1)\lambda)$, using steps $(\mu(\mathfrak{G}) - 1, 0)$ or $(0, 1)$, such that q never passes above the line $x = y$,

(f) the number of ways of dissecting a convex $(\lambda(\mu(\mathfrak{G}) - 1) + 2)$-gon into λ convex $(\mu(\mathfrak{G}) + 1)$-gons, by drawing diagonals which do not intersect in their interiors;

cf. [33, Proposition 6.2.1]. If we deform the (x, y)-plane by means of the transformation

$$x' = (\mu(\mathfrak{G}) - 1)\lambda - y, \quad y' = \lambda - \frac{x}{\mu(\mathfrak{G}) - 1},$$

then we find from (e) that $(-1)^{(\mu(\mathfrak{G})-1)\lambda+1}\big\langle z^\lambda \mid \widehat{X}_q^*(z)\big\rangle$ (and hence $f_\lambda(\mathfrak{G})$ modulo 2) also equals

(g) the number of lattice paths q in the 2-dimensional integral lattice $\mathbb{Z}^2$ starting in the origin $(0, 0)$ and terminating in the lattice point $((\mu(\mathfrak{G}) - 1)\lambda, \lambda)$, such that (i) q consists only of positive horizontal and vertical unit steps, and (ii) q never passes above the line $x = (\mu(\mathfrak{G}) - 1)y$. [13]

References

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

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

[3] D. E. Cohen, Groups with free subgroups of finite index, in: *Proceedings of the Conference on Group Theory (University of Wisconsin-Parkside 1972)*, Lecture Notes in Mathematics Vol. 319, Springer, 1973, 26–44.

[4] H. Delange, Sur la fonction sommatoire de la fonction 'Somme de chiffre', *Enseign. Math.* II Sér. **21** (1975), 31–47.

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

[6] M. Grady and M. Newman, Counting subgroups of given index in Hecke groups, *Contemporary Math.* **143** (1993), 431–436.

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

[8] M. Grady and M. Newman, Residue periodicity in subgroup counting functions, *Contemporary Math.* **166** (1994), 265–273.

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

[10] W. Imrich, On the number of subgroups of a given index in $SL_2(\mathbb{Z})$, *Archiv d. Math.* **31** (1978), 224–231.

[13] Cf. [14, pp. 8–9]. See also [29, Chapter I] for related results concerning the enumeration of lattice paths.

[11] A. Karrass, A. Pietrowski, and D. Solitar, Finite and infinite cyclic extensions of free groups, *J. Austral. Math. Soc.* **16** (1973), 458–466.
[12] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. reine u. angew. Math.* **44** (1852), 93–146. Reprinted in: Collected Papers (edited by A. Weil), Vol. I, 485–538, Springer, New York, 1975.
[13] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, Birkhäuser, Basel, 2003.
[14] S. G. Mohanti, *Lattice path counting and applications*, Academic Press, New York, 1979.
[15] T. Müller, Kombinatorische Aspekte endlich erzeugter virtuell freier Gruppen, Ph. D. Thesis, Universität Frankfurt am Main, 1989.
[16] T. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.
[17] T. Müller, A group-theoretical generalization of Pascal's triangle, *Europ. J. Combin.* **12** (1991), 43–49.
[18] T. Müller, Counting free subgroups of finite index, *Archiv d. Math.* **59** (1992), 525–533.
[19] T. Müller, Subgroup growth of free products, *Invent. Math.* **126** (1996), 111–131.
[20] T. Müller, Combinatorial classification of finitely generated virtually free groups, *J. Algebra* **195** (1997), 285–294.
[21] T. Müller, Finite group actions and asymptotic expansion of $e^{P(z)}$, *Combinatorica* **17** (1997), 523–554.
[22] T. Müller, Remarks on the PhD thesis of A. Meyer, unpublished manuscript, 1998.
[23] T. Müller, Enumerating representations in finite wreath products, *Adv. in Math.* **153** (2000), 118–154.
[24] T. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, *Bull. London Math. Soc.* **34** (2002), 587–598.
[25] T. Müller, Parity patterns in Hecke groups and Fermat primes, in: *Proceedings of the conference 'Groups: Topological, Combinatorial and Arithmetic Aspects' (Bielefeld 1999)*, LMS Lecture Notes Series, Cambridge University Press, to appear.
[26] T. Müller (editor), *Proceedings of the conference 'Groups: Topological, Combinatorial and Arithmetic Aspects' (Bielefeld 1999)*, LMS Lecture Notes Series, Cambridge University Press, to appear.
[27] T. Müller, Modular subgroup arithmetic, in: *Proceedings of the 2001 Durham Symposium on Groups, Combinatorics and Geometries*, World Scientific, to appear.
[28] T. Müller, Modular subgroup arithmetic in free products, *Forum Math.*, in press.
[29] T. V. Narayana, *Lattice path combinatorics with statistical applications*, Math. Expositions No. 23, University of Toronto Press, London, 1979.
[30] G. P. Scott, An embedding theorem for groups with a free subgroup of finite index, *Bull. London Math. Soc.* **6** (1974), 304–306.
[31] J.–P. Serre, *Trees*, Springer, Berlin–Heidelberg–New York, 1980.
[32] J. Stallings, On torsion-free groups with infinitely many ends, *Ann. of Math.* **88** (1968), 312–334.
[33] R. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge University Press, New York, 1999.
[34] W. Stothers, The number of subgroups of given index in the modular group, *Proc. Royal Soc. Edinburgh* **78A** (1977), 105–112.
[35] W. Stothers, Free subgroups of the free product of cyclic groups, *Math. Comp.* **32** (1978), 1274–1280.
[36] C.T.C. Wall, Poincaré complexes: I, *Ann. of Math.* **86** (1967), 213–245.

School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK (T.W.Muller@qmul.ac.uk)

Jan-Christoph Schlage-Puchta, Mathematisches Institut, Albert-Ludwigs-Universität, Eckerstr. 1, 79104 Freiburg, Germany (jcp@math.uni-freiburg.de)