PARITY PATTERNS IN ONE-RELATOR GROUPS

Thomas W. Müller and Jan-Christoph Puchta

Abstract. We investigate the behaviour modulo 2 of the number $s_n(\Gamma)$ of index n subgroups in one-relator groups Γ. Among other things we show that, for a substantial class of one-relator groups Γ (including in particular all surface groups), $s_n(\Gamma)$ is intimately connected with representation numbers of binary quadratic forms, and that $s_n(\Gamma)$ is odd if and only if n is a square or twice a square. The proofs make use of parity properties of character values and multiplicities for symmetric groups, which appear to be of independent interest.

1. Introduction and main results

For a finitely generated group Γ denote by $s_n(\Gamma)$ the number of subgroups of index n in Γ. The present paper is concerned with the behaviour modulo 2 of the function $s_n(\Gamma)$ in the case when Γ is a one-relator group. Among other things we show that, for a substantial class of one-relator groups Γ containing in particular all surface groups, the parity pattern of $s_n(\Gamma)$ is intimately connected with representation numbers of binary quadratic forms, and can be determined in closed form.

The natural framework for our research is the theory of *subgroup growth* of finitely generated groups. The notion of subgroup growth, which has evolved over the last two decades in the work of Grunewald, Lubotzky, Mann, Segal, and others including the first named of the present authors, brings together under a common conceptual roof investigations concerning arithmetic properties of the sequence $\{s_n(\Gamma)\}_{n\geq 1}$ or related subgroup counting functions and their connection with the algebraic structure of the underlying group Γ. The original motivation for these studies comes from three sources: the notion of word growth and, more specifically, Gromov's characterization in [7] 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. [8], [9], and [10]. Some of the major developments up to 1992 are described in Lubotzky's Galway notes [17], [18], and the literature cited therein. More recent contributions include [4], [20], [19], [21], [22], [23], [28], [29], and [5].

We will work over the alphabet $\mathcal{A} = \{x_1, x_2, \ldots, x_1^{-1}, x_2^{-1}, \ldots\}$. Define two classes of words $\mathcal{W}_1$, $\mathcal{W}_2$ over $\mathcal{A}$ as follows.

(i)$_1$ $x_i^2, [x_i, x_j] \in \mathcal{W}_1$ for all $i, j \in \mathbb{N}$ and $i \neq j$.

(i)$_2$ $x_i^k \in \mathcal{W}_2$ for all $i, k \in \mathbb{N}$.

(ii)$_j$ If $w_1, w_2 \in \mathcal{W}_j$ have no generator in common, then $w_1 w_2 \in \mathcal{W}_j$.

(iii)$_j$ If $v \in \mathcal{W}_j$, and x_i is a generator not occurring in v, then $[v, x_i] \in \mathcal{W}_j$.

(iv)$_j$ $\mathcal{W}_j$ is the smallest set of words over $\mathcal{A}$ satisfying (i)$_j$, (ii)$_j$, and (iii)$_j$.

Clearly, all surface group relators

$$\prod_{i=1}^{g} [x_{2i-1}, x_{2i}] \quad \text{and} \quad \prod_{i=1}^{h} x_i^2, \quad g, h \geq 1$$

are contained in $\mathcal{W}_1$, as is, for instance, the word $w = [x_1^2 x_2^2, x_3]$, and $\mathcal{W}_1 \subsetneq \mathcal{W}_2$. For a word $w = w(x_1, \ldots, x_d)$ over $\mathcal{A}$ involving the generators $x_1, \ldots, x_d$, define the one-relator group Γ_w *associated with* w via

$$\Gamma_w = \Big\langle x_1, x_2, \ldots, x_d \mid w(x_1, \ldots, x_d) = 1 \Big\rangle.$$

Our first main result describes the behaviour modulo 2 of $s_n(\Gamma_w)$ for words $w \in \mathcal{W}_1$.

Theorem 1. *If w is in $\mathcal{W}_1$ and involves at least three generators, then $s_n(\Gamma_w)$ is odd if and only if $n = k^2$ or $n = 2k^2$ for some $k \geq 1$; in particular, all groups Γ_w with $w \in \mathcal{W}_1$ involving three or more generators share the same parity pattern, and $s_n(\Gamma_w)$ is multiplicative modulo 2.*

It appears likely that Theorem 1 is best possible in the sense that if for some $w \in \mathcal{W}_2$ the function $s_n(\Gamma_w)$ displays the parity pattern described in Theorem 1, then in fact $w \in \mathcal{W}_1$. Concerning the larger class $\mathcal{W}_2$ we are able to show the following.

Theorem 2. *Let w be a word in $\mathcal{W}_2$ involving three or more generators. Then*
(a) *the sequence $s_n(\Gamma_w)$ is ultimately periodic modulo 2 if and only if it is periodic,*
(b) *the function $\mathcal{S}_w(x)$ given by*

$$\mathcal{S}_w(x) := \big|\{n \leq x : \ s_n(\Gamma_w) \equiv 0 \ (2)\}\big|, \quad x \geq 1$$

satisfies

$$\limsup_{x \to \infty} \frac{\mathcal{S}_w(x) \log_2(x)}{\sqrt{x}} \geq \frac{1}{4}, \tag{1}$$

or $\mathcal{S}_w(x)$ is identically zero.

The key to Theorems 1 and 2 lies in a remarkable recurrence relation for the mod 2 behaviour of $s_n(\Gamma_w)$ with $w \in \mathcal{W}_2$, which we describe next.

Theorem 3. *Let $w \in \mathcal{W}_2$ be a word involving three or more generators. Then there is a sequence $\{\alpha_k\} \in \{0,1\}^{\mathbb{N}}$, such that $\alpha_1 = 1$ and*

$$s_n(\Gamma_w) \equiv \sum_{\substack{k \geq 1 \\ k(k+1) < 2n}} \alpha_k \, s_{n - k(k+1)/2}(\Gamma_w) \ + \ \delta(n) \mod 2, \quad n \geq 1, \tag{2}$$

where

$$\delta(n) = \begin{cases} 1, & n = \frac{k(k+1)}{2} \text{ with } n \text{ odd and } \alpha_k = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, if $w \in \mathcal{W}_1$, then $\alpha_k = 1$ for all $k \geq 1$.

Apart from their intrinsic value, Theorems 1-3 also appear to be of some general interest within the theory of subgroup growth: they add a surprising new feature to our as yet fragmentary knowledge of modular properties of subgroup counting functions [1] and, in conjunction with the asymptotic estimate for surface groups established in [30], they form what might become the beginning of a systematic theory for the subgroup growth of one-relator groups. In the next two sections, Theorems 1 respectively 2 are deduced from Theorem 3, while the proof of Theorem 3 occupies sections 4 – 6.

2. Proof of Theorem 1

We shall use induction on n, the case $n = 1$ being trivial. In what follows, it will be convenient to abbreviate the statement 'n is a square' as '$n = \square$'; similarly, '$n = 2\square$' will be short-hand notation for the statement that 'n equals twice a square'. Moreover, for a number c and a condition φ we will use the notation $\{c \mid \varphi\}$, meaning that this symbol has the value c if φ holds and 0 otherwise. Assuming that

$$s_n(\Gamma_w) \equiv 1\ (2) \Leftrightarrow n = \square \text{ or } n = 2\square, \quad n < N$$

for some $N \geq 2$, the recurrence relation (2) together with an obvious transformation gives that modulo 2

$$\begin{aligned} s_N(\Gamma_w) &\equiv \Big|\Big\{(x,y) \in \mathbb{N}^2 :\ N = x^2 + \frac{y(y+1)}{2}\Big\}\Big| \\ &\qquad + \Big|\Big\{(x,y) \in \mathbb{N}^2 :\ N = 2x^2 + \frac{y(y+1)}{2}\Big\}\Big| + \delta(N) \\ &\equiv \Big|\Big\{(x,y) :\ 8N+1 = 2x^2 + y^2, x > 0, y > 1\Big\}\Big| \\ &\qquad + \Big|\Big\{(x,y) :\ 8N+1 = x^2 + y^2, 2 \mid x, x > 0, y > 1\Big\}\Big| + \delta(N). \end{aligned}$$

For $n \in \mathbb{N}$, define

$$\begin{aligned} R_1(n) &:= \Big|\Big\{(x,y) \in \mathbb{Z}^2 :\ n = 2x^2 + y^2\Big\}\Big| \\ R_2(n) &:= \Big|\Big\{(x,y) \in \mathbb{Z}^2 :\ n = x^2 + y^2, 2 \mid x\Big\}\Big|. \end{aligned}$$

Then

$$\begin{aligned} s_N(\Gamma_w) \equiv \frac{1}{4}\Big[R_1(8N+1) + R_2(8N+1) - \big\{4 \mid 8N+1 = \square\big\} - \big\{4 \mid N = \square\big\} \\ - \big\{4 \mid N = 2\square\big\}\Big] + \delta(N) \mod 2. \quad (3) \end{aligned}$$

The representation numbers of binary quadratic forms have been computed by Legendre, and independently by Gauss; cf. [6, § 205], [15], and [2, Chap. VI.8]. Applying Legendre's and Gauss' result, and writing the prime decomposition of n as

[1] Cf. [24], [25], [26], and [27] for the present state of affairs concerning modular subgroup arithmetic.

$n = \prod_p p^{a_p(n)}$, we find that for n odd

$$R_1(n) = \begin{cases} 2 \prod\limits_{p \equiv 1,3\,(8)} \big(a_p(n)+1\big), & a_p(n) \equiv 0\ (2) \text{ for } p \equiv 5,7\ (8) \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

$$R_2(n) = \begin{cases} 2 \prod\limits_{p \equiv 1\,(4)} \big(a_p(n)+1\big), & a_p(n) \equiv 0\ (2) \text{ for } p \equiv 3\ (4) \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Such formulae can also be deduced from results concerning the decomposition of rational primes in quadratic number fields; cf. for instance [11, Satz 89]. Write $8N+1 = u^2 v$ with v square-free, and suppose first that $v = 1$. Then (3) takes the form

$$s_N(\Gamma_w) \,-\, \big\{1 \mid N = \square\big\} \,-\, \big\{1 \mid N = 2\square\big\} \equiv \frac{1}{4}\big[R_1(8N+1) + R_2(8N+1)\big] + \delta(N) + 1 \mod 2.$$

Using (4) and (5), the right-hand side becomes modulo 2

$$\frac{1}{2}\Big[\prod_{p\equiv 1,3\,(8)} \big(2a_p(u)+1\big) \,+\, \prod_{p\equiv 1\,(4)} \big(2a_p(u)+1\big)\Big] \,+\, \delta(N) \,+\, 1 \equiv \sum_{p\equiv 3,5\,(8)} a_p(u) \,+\, \delta(N).$$

Decomposing u in the form

$$u \equiv 3^{\sum_{p\equiv 3\,(8)} a_p(u)} \cdot 5^{\sum_{p\equiv 5\,(8)} a_p(u)} \cdot 7^{\sum_{p\equiv 7\,(8)} a_p(u)} \mod 8,$$

we see that $\sum_{p\equiv 3,5\,(8)} a_p(u)$ is odd if and only if $u \equiv 3, 5 \bmod 8$. On the other hand, $\delta(N) = 1$ if and only if N is odd, since in this case N is automatically triangular, the latter condition being equivalent to $u \equiv 3, 5 \bmod 8$. Hence, for $8N+1$ a square, (3) takes the form

$$s_N(\Gamma_w) \equiv \big\{1 \mid N = \square\big\} \,+\, \big\{1 \mid N = 2\square\big\} \mod 2,$$

proving our claim in this case. Now let $v > 1$. Then (3) simplifies to

$$s_N(\Gamma_w) - \big\{1 \mid N = \square\big\} - \big\{1 \mid N = 2\square\big\} \equiv \frac{1}{4}\Big[R_1(8N+1) + R_2(8N+1)\Big] \mod 2. \tag{6}$$

Assume that v is not prime. We claim that this implies $R_i(8N+1) \equiv 0 \bmod 8$. Indeed, either $R_i(8N+1) = 0$, because $8N+1$ is divisible by some prime p with $R_i(p) = 0$ and $a_p(8N+1) \equiv 1 \bmod 2$, or in the product evaluations for $R_i(8N+1)$ given in (4), (5) there occur at least two even factors, implying $R_i(8N+1) \equiv 0 \bmod 8$. Finally, if v is prime, then $v \equiv 1 \bmod 8$, and in the product evaluations for $R_1(8N+1)$ and $R_2(8N+1)$ precisely one term is even, implying $R_1(8N+1) \equiv R_2(8N+1) \equiv 4 \bmod 8$. Hence, whether v is prime or composite, we always have $R_1(8N+1) + R_2(8N+1) \equiv 0 \bmod 8$, and the right-hand side of (6) is even, proving our claim in the case $v > 1$ as well.

3. Proof of Theorem 2

(i) Let $w \in \mathcal{W}_2$ be a word involving $d \geq 3$ generators, and suppose that $s_n(\Gamma_w)$ is ultimately periodic modulo 2 with period ν, say. Choose an integer $k_0 \geq 2\nu$ such that $s_n(\Gamma_w) \equiv s_{n-\nu}(\Gamma_w)$ (2) for $n > k_0$, and put $n_0 := \frac{k_0(k_0+1)}{2} + 1$. As $d \geq 3$, the recurrence relation (2) gives

$$s_{n_0}(\Gamma_w) \equiv \sum_{\substack{k\geq 1 \\ k(k+1)<2n_0}} \alpha_k \, s_{n_0-k(k+1)/2}(\Gamma_w) \mod 2,$$

but also

$$s_{n_0}(\Gamma_w) \equiv s_{n_0-\nu}(\Gamma_w) \equiv \sum_{\substack{k\geq 1 \\ k(k+1)<2(n_0-\nu)}} \alpha_k \, s_{n_0-k(k+1)/2-\nu}(\Gamma_w) \, + \, \delta(n_0-\nu) \mod 2.$$

Since

$$(k_0-1)k_0 = k_0(k_0+1) - 2k_0 \leq k_0(k_0+1) - 2\nu < 2(n_0-\nu)$$

and

$$k_0(k_0+1) = 2(n_0-1) \geq 2(n_0-\nu),$$

the two sums range over $1 \leq k \leq k_0$ respectively $1 \leq k < k_0$, and as

$$n_0 - \frac{(k_0-1)k_0}{2} = k_0 + 1 > k_0,$$

we have

$$s_{n_0-k(k+1)/2-\nu}(\Gamma_w) \equiv s_{n_0-k(k+1)/2}(\Gamma_w) \mod 2, \quad 1 \leq k < k_0.$$

Hence, the two sums differ precisely in the term

$$\alpha_{k_0} \, s_{n_0-k_0(k_0+1)/2}(\Gamma_w) + \delta(n_0-\nu) = \alpha_{k_0} + \delta(n_0-\nu),$$

which forces $\alpha_{k_0} + \delta(n_0-\nu) \equiv 0$ (2). If $\nu > 1$, then

$$\frac{(k_0-1)k_0}{2} < n_0 - \nu < \frac{k_0(k_0+1)}{2},$$

hence $\delta(n_0-\nu) = 0$ and $\alpha_{k_0} = 0$ in this case. Since every integer $k \geq k_0$ satisfies the same hypotheses as k_0, our argument gives $\alpha_k = 0$ for $k \geq k_0$, provided $\nu > 1$. Taking into account that $\alpha_1 = 1$, this implies periodicity of $s_n(\Gamma_w)$; cf. for instance [16, Theorem 8.11]. Now suppose that $\nu = 1$. Every multiple of a period being again a period, by what we have shown so far, $s_n(\Gamma_w)$ is periodic modulo 2 with periods 2 and 3. But this implies that $s_n(\Gamma_w)$ is constant modulo 2.

(ii) Assume first that $\alpha_k = 0$ for all but finitely many k. Then the sequence $s_n(\Gamma_w)$ is periodic modulo 2 by [16, Theorem 8.11], hence either $\mathcal{S}_w(x) = 0$, or $\mathcal{S}_w(x) \gg x$; in particular our claim holds. Now suppose that $\alpha_k = 1$ for infinitely many k. For $x \geq 1$ define counting functions

$$A(x) := \big|\big\{k : \; k(k+1) < 2x, \, \alpha_k = 1\big\}\big|$$

$$B(x) := \big|\big\{n \leq x : \; A(n) \equiv 0 \; (2), \, n \text{ not triangular}\big\}\big|.$$

If n is an integer counted by $B(x)$, then $s_n(\Gamma_w)$ is even if and only if the set

$$\Big\{k:\ k(k+1)<2n,\ \alpha_k=1,\ s_{n-k(k+1)/2}(\Gamma_w)\equiv 0\ (2)\Big\}$$

has even cardinality; in particular, $s_n(\Gamma_w)$ is even if this set is empty. It follows that

$$\begin{aligned}\mathcal{S}_w(x) &\geq \Big|\Big\{n\leq x:\ A(n)\equiv 0\ (2),\ n \text{ not triangular}\Big\}\Big| \\ &\qquad - \Big|\Big\{n\leq x:\ \exists k:\ \alpha_k=1,\ s_{n-k(k+1)/2}(\Gamma_w)\equiv 0\ (2)\Big\}\Big| \\ &\geq B(x)-\mathcal{S}(x)A(x),\end{aligned}$$

that is

$$\mathcal{S}_w(x)\geq \frac{B(x)}{1+A(x)}.$$

If $\frac{x}{2}\leq \frac{k(k+1)}{2}\leq x$ and $A(\frac{k(k+1)}{2})\equiv 0\ (2)$, then $A(n)\equiv 0\ (2)$ for all $n\in[\frac{k(k+1)}{2},\frac{(k+1)(k+2)}{2}-1]$, the interval containing at least $\sqrt{x}$ integral points. Hence, we obtain the estimates

$$B(x)\geq \sqrt{x}\,\frac{A(x)-A(\frac{x}{2})-1}{2},\quad x\geq 1,$$

and

$$B(x_\nu)\geq\sqrt{x_\nu} \tag{7}$$

for a sequence x_ν tending to infinity. Now we distinguish two cases. If

$$\limsup_{x\to\infty}\big(A(x)-A(\tfrac{x}{2})\big)\geq 2,$$

then we can find a sequence x_ν tending to infinity and a constant y_0 such that

$$A(x_\nu)-A(\tfrac{x_\nu}{2})\geq 2\ \text{ and }\ A(x_\nu)-A(\tfrac{x_\nu}{2})\geq A(y)-A(\tfrac{y}{2}),\ y_0\leq y\leq x_\nu.$$

Hence, we obtain

$$\begin{aligned}\mathcal{S}_w(x_\nu)&\geq \frac{B(x_\nu)}{1+A(x_\nu)}\\ &\geq \frac{\sqrt{x_\nu}\big(A(x_\nu)-A(\frac{x_\nu}{2})-1\big)}{2\big(A(x_\nu)-A(\frac{x_\nu}{2})\big)\log_2 x_\nu+y_0+1}\\ &\geq \Big(\frac14+o(1)\Big)\frac{\sqrt{x_\nu}}{\log_2 x_\nu}.\end{aligned}$$

If, on the other hand,

$$A(x)-A(\frac{x}{2})\leq 1,\quad x>x_0,$$

then $A(x)\leq \log_2 x+x_0$, and if x_ν runs through a sequence as in (7), then

$$\mathcal{S}_w(x_\nu)\geq\frac{B(x_\nu)}{1+A(x_\nu)}\geq\frac{\sqrt{x_\nu}}{\log_2 x_\nu+x_0+1}=\big(1+o(1)\big)\frac{\sqrt{x_\nu}}{\log_2 x_\nu}.$$

We conclude that in each case

$$\mathcal{S}_w(x_\nu)\geq\Big(\frac14+o(1)\Big)\frac{\sqrt{x_\nu}}{\log_2 x_\nu}$$

for a suitably chosen sequence $x_\nu \to \infty$, and (1) follows.

4. The coefficients $\alpha_\chi(w)$

Let $w = w(x_1, \dots, x_d)$ be a word over $\mathcal{A}$ involving the generators $x_1, \dots, x_d$, and let χ be an irreducible character of S_n. Define numbers $\alpha_\chi(w) \in \mathbb{C}$ by means of the expansion

$$\begin{aligned} N_w(\pi) :&= \left|\left\{(x_1, \dots, x_d) \in S_n^d : \ w(x_1, \dots, x_d) = \pi\right\}\right| \\ &= (n!)^{d-1} \sum_{\chi \in \mathrm{Irr}(S_n)} \alpha_\chi(w)\chi(\pi), \quad \pi \in S_n. \end{aligned}$$

Note that $N_w(\pi)$ is a class function, hence the coefficients $\alpha_\chi(w)$ are well defined. Our first lemma provides information concerning the $\alpha_\chi(w)$, leading in particular to the explicit computation of these coefficients for each word $w \in \mathcal{W}_1$ and all χ.

Lemma 1. *Let w_1, w_2, v be words over $\mathcal{A}$, and let χ be an irreducible character of S_n.*

(i) *We have $\alpha_\chi(x_i^2) = 1$, $\alpha_\chi(x_i^k) \in \mathbb{N}_0$, and $\alpha_\chi([x_i, x_j]) = \frac{1}{\chi(1)}$ for all $i, j, k \in \mathbb{N}$.*

(ii) *If w_1 and w_2 have no generator in common, then we have*

$$\alpha_\chi(w_1 w_2) = \frac{\alpha_\chi(w_1)\,\alpha_\chi(w_2)}{\chi(1)}.$$

(iii) *If x_i does not occur among the generators of v, then*

$$\alpha_\chi([v, x_i]) = \frac{1}{\chi(1)} \sum_{\chi' \in \mathrm{Irr}(S_n)} \alpha_{\chi'}(v)\,\langle \chi^2 \mid \chi' \rangle.$$

Proof. (i) The first two claims restate the facts that the root number functions of S_n are proper characters, and that the square root function is the model character of S_n; cf. [31] and [14, Chap. 6.2]. The last claim follows from the formula (see [30, Lemma 1])

$$N_{[x,y]}(\pi) = n! \sum_\chi \frac{\chi(\pi)}{\chi(1)}, \quad \pi \in S_n.$$

(ii) We shall use the fact that, for any two conjugacy classes C_1, C_2 in a finite group G, the number of solutions of the equation $x_1 \cdot x_2 = g$ with $x_i \in C_i$ equals

$$\frac{|C_1||C_2|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C_1)\chi(C_2)\chi(g^{-1})}{\chi(1)}; \tag{8}$$

cf. for instance [1, Prop. 9.33] or [14, Theorem 6.3.1]. Suppose that $w = w_1 w_2$ involves precisely d generators. Then, using (8) and orthogonality, as well as the fact that the

characters of symmetric groups are real, we find that

$$\begin{aligned} N_w(\pi) &= (n!)^{-1} \sum_{C_1,C_2} \sum_{\chi} |C_1||C_2| N_{w_1}(C_1) N_{w_2}(C_2) \frac{\chi(C_1)\chi(C_2)\chi(\pi)}{\chi(1)} \\ &= (n!)^{d-3} \sum_{\chi_1,\chi_2,\chi_3} \frac{\alpha_{\chi_2}(w_1)\alpha_{\chi_3}(w_2)\chi_1(\pi)}{\chi_1(1)} \Big(\sum_{C_1} |C_1| \chi_1(C_1)\chi_2(C_1) \Big) \\ &\qquad \times \Big(\sum_{C_2} |C_2| \chi_1(C_2)\chi_3(C_2) \Big) \\ &= (n!)^{d-1} \sum_{\chi} \frac{\alpha_\chi(w_1)\alpha_\chi(w_2)}{\chi(1)} \chi(\pi), \end{aligned}$$

which proves our claim.

(iii) Rewriting the equation $[x, y] = \pi$ as $x^{-1} \cdot x^y = \pi$ shows that the number of solutions in S_n of this equation can be obtained by solving the equation $a \cdot b = \pi$ with a and b conjugate, and counting each solution with weight $|C_{S_n}(a)|$. Hence, using (8) again, we see that for $w = [v(x_1, \ldots, x_{d-1}), x_d]$

$$\begin{aligned} N_w(\pi) &= \sum_{C} \sum_{\chi} \frac{|C|^2}{n!} \frac{(\chi(C))^2 \chi(\pi)}{\chi(1)} \frac{n!}{|C|} N_v(C) \\ &= (n!)^{d-2} \sum_{\chi_1,\chi_2} \frac{\alpha_{\chi_2}(v)\chi_1(\pi)}{\chi_1(1)} \sum_{C} |C| (\chi_1(C))^2 \chi_2(C) \\ &= \frac{(n!)^{d-1}}{\chi(1)} \sum_{\chi} \Big[\sum_{\chi'} \alpha_{\chi'}(v) \langle \chi^2 \mid \chi' \rangle \Big] \chi(\pi) \end{aligned}$$

as claimed. □

5. Two lemmas

Denote by σ the bijection between the self-conjugate partitions of n and the partitions of n into distinct odd parts, mapping a self-conjugate partition λ onto the partition given by the symmetric hooks of λ (with respect to the diagonal). Moreover, denote by C_λ the conjugacy class of S_n whose cycle structure is given by the partition $\lambda \vdash n$, and by χ_λ the irreducible character of S_n associated with λ. The sign character $\chi_{(1^n)}$ will be denoted by ε_n.

Lemma 2. *Let λ_1, λ_2 be partitions of n with λ_1 self-conjugate. Then $\chi_{\lambda_1}(C_{\lambda_2})$ is odd if and only if $\lambda_2 = \lambda_1^\sigma$.*

Proof. Note that since $\pi \sim \pi^a$ for all $\pi \in S_n$ and exponents a coprime to the order of π, characters of S_n are integer-valued. We prove the statement by induction on n, the case $n = 1$ being trivial. Assume our claim to be true for all $n < N$, and let λ_1, λ_2 be

partitions of N with λ_1 self-conjugate. Furthermore, let ℓ be some part of λ_2, and let $h_1, \ldots, h_k$ be the hooks of length ℓ in λ_1. By the Murnagham-Nakayama rule,

$$\chi_{\lambda_1}(C_{\lambda_2}) \equiv \sum_{i=1}^{k} \chi_{\lambda_1 \setminus h_i}(C_{\lambda_2 \setminus \ell}) \mod 2. \tag{9}$$

Since λ_1 is self-conjugate, reflection in the main diagonal induces a bijection on the set $\{h_1, \ldots, h_k\}$ fixing precisely the symmetric hook of length ℓ (if there is one). Since for a partition $\mu \vdash N - \ell$ we have $\chi_{\mu'} = \varepsilon_{N-\ell}\chi_\mu$, the contribution to the right-hand side of (9) of hooks which are not symmetric vanishes modulo 2. Consequently, if λ_1 has no symmetric hook of length ℓ, then $\chi_{\lambda_1}(C_{\lambda_2})$ is even, and $\lambda_1^\sigma \neq \lambda_2$, i.e., our claim holds in this case. If, on the other hand, λ_1 has a symmetric hook of length ℓ, then it is uniquely determined, h_1 say, and (9) gives

$$\chi_{\lambda_1}(C_{\lambda_2}) \equiv \chi_{\lambda_1 \setminus h_1}(C_{\lambda_2 \setminus \ell}) \mod 2. \tag{10}$$

The partition $\lambda_1 \setminus h_1$ is again symmetric and of weight $N - \ell$, and our inductive hypothesis ensures that the right-hand side of (10) is odd if and only if $(\lambda_1 \setminus h_1)^\sigma = \lambda_2 \setminus \ell$. The latter condition is easily seen to be equivalent to $\lambda_1^\sigma = \lambda_2$, and we conclude that indeed $\chi_{\lambda_1}(C_{\lambda_2}) \equiv 1\ (2)$ if and only if $\lambda_1^\sigma = \lambda_2$. □

Call an irreducible character χ of S_n *symmetric*, if $\chi = \varepsilon_n \chi$; this is equivalent to demanding that the partition associated with χ be self-conjugate.

Lemma 3. *Let χ, χ' be irreducible characters of S_n.*

(i) *If χ is symmetric, then $\langle \chi^{2^k} \mid \chi' \rangle = \langle \chi^{2^k} \mid \varepsilon_n \chi' \rangle$ for all k.*

(ii) *If both χ and χ' are symmetric, then $\langle \chi^2 \mid \chi' \rangle$ is odd if and only if $\chi = \chi'$.*

Proof. (i) Since χ is symmetric, we have for $k \geq 0$

$$\langle \chi^{2^k} \mid \chi' \rangle = \langle \chi \mid \chi^{2^k - 1} \chi' \rangle = \langle \varepsilon_n \chi \mid \chi^{2^k - 1} \chi' \rangle = \langle \chi^{2^k} \mid \varepsilon_n \chi' \rangle.$$

(ii) We will work in the GF(2)-algebra $\mathfrak{A} = \mathrm{GF}(2)[\mathrm{Irr}(S_n)]$ generated by the irreducible characters of S_n. The scalar product of characters extends naturally to a GF(2)-valued bilinear form on $\mathfrak{A}$. Define a matrix $\mathcal{M} = (M_{\chi\chi'})_{\chi,\chi' \in \mathrm{Irr}(S_n)}$ via $M_{\chi\chi'} := \langle \chi^2 \mid \chi' \rangle$. For $\psi \in \mathfrak{A}$ we have

$$\begin{aligned} \psi^2 &= \Big(\sum_{\chi \in \mathrm{Irr}(S_n)} \langle \psi \mid \chi \rangle \chi \Big)^2 \\ &= \sum_{\chi \in \mathrm{Irr}(S_n)} \langle \psi \mid \chi \rangle^2 \chi^2 \ + \ 2 \sum_{\chi \neq \chi'} \langle \psi \mid \chi \rangle \langle \psi \mid \chi' \rangle \chi \chi' \\ &= \sum_{\chi, \chi'} \langle \psi \mid \chi \rangle \langle \chi^2 \mid \chi' \rangle \chi'. \end{aligned}$$

On the other hand,

$$\mathcal{M}\big(\langle \psi \mid \chi \rangle\big)_{\chi \in \mathrm{Irr}(S_n)} = \Big(\sum_{\chi} \langle \psi \mid \chi \rangle \langle \chi^2 \mid \chi' \rangle \Big)_{\chi' \in \mathrm{Irr}(S_n)},$$

i.e., defining the action of $\mathcal{M}$ on $\mathfrak{A}$ via matrix multiplication applied to coefficient vectors, we have $\mathcal{M}\psi = \psi^2$. Induction on k gives $\mathcal{M}^k\psi = \psi^{2^k}$ for all $k \geq 1$ and $\psi \in \mathfrak{A}$; in particular, we have $\langle \mathcal{M}^k\chi \mid \chi' \rangle = \langle \chi^{2^k} \mid \chi' \rangle$, i.e., the (χ, χ')-entry of the matrix $\mathcal{M}^k$ is $\langle \chi^{2^k} \mid \chi' \rangle$. We now arrange the rows and columns of $\mathcal{M}$ as follows: a first block of rows (columns) indexed by the symmetric characters of S_n is followed by a block of rows (columns) labelled by those characters χ_λ which satisfy $\lambda > \lambda'$ in the lexicographical ordering. The labels of the remaining rows (columns) are then obtained from the latter labels by multiplication with the sign character. We claim that, with this labelling of rows and columns, $\mathcal{M}^k$ takes the form

$$\mathcal{M}^k = \left(\begin{array}{c|c|c} A^{(k)} & B^{(k)} & B^{(k)} \\ \hline C^{(k)} & D^{(k)} & \\ \hline C^{(k)} & D^{(k)} & \end{array}\right),$$

where the square matrix $A^{(k)}$ contains all entries of $\mathcal{M}^k$ labelled by pairs (χ, χ') with both χ and χ' symmetric. Indeed, the duplication of $B^{(k)}$ in the first row of this block matrix comes from the first part of the lemma, while the duplication of $C^{(k)}$ and $D^{(k)}$ stems from the equation $\langle \chi^{2^k} \mid \chi' \rangle = \langle (\varepsilon_n\chi)^{2^k} \mid \chi' \rangle$, which holds trivially for all χ, χ' and $k \geq 1$. Next, we use Lemma 2 to compute $A^{(k)}$ for k sufficiently large, $2^k > n$, say. We have

$$A^{(k)}_{\chi\chi'} = \langle \chi^{2^k} \mid \chi' \rangle = \frac{1}{n!} \sum_C |C| \chi^{2^k}(C)\chi'(C) \bmod 2.$$

Assume that $\chi \neq \chi'$. We will show that the integer

$$\sum_C \frac{|C|}{n!} \chi^{2^k}(C)\chi'(C) \tag{11}$$

is even, by proving that every single term is a rational number with positive 2-exponent. First consider a class C such that $\chi(C)$ is even. Then $\chi^{2^k}(C)$ is divisible by 2^{2^k}, while $n!$ is not divisible by 2^n. Since $|C|, \chi'(C)$ are integral and $2^k > n$, the 2-exponent of such a term is indeed positive. Now suppose that $\chi(C)$ is odd, and set $\chi = \chi_\lambda$, $\chi' = \chi_\mu$ with partitions $\lambda, \mu \vdash n$. By Lemma 2, $\chi_\lambda(C)$ is odd if and only if $C = C_{\lambda^\sigma}$, hence we only have to consider the single term

$$\frac{|C_{\lambda^\sigma}|}{n!} \chi_\lambda^{2^k}(C_{\lambda^\sigma})\chi'_\mu(C_{\lambda^\sigma}). \tag{12}$$

Write $\lambda^\sigma = (\lambda_1^\sigma, \lambda_2^\sigma, \ldots, \lambda_\ell^\sigma)$ with odd and pairwise distinct parts λ_i^σ. Then $|C_{\lambda^\sigma}| = \frac{n!}{\lambda_1^\sigma \cdots \lambda_\ell^\sigma}$ contains the same 2-part as $n!$, i.e., $\frac{|C_{\lambda^\sigma}|}{n!}$ is a rational number with 2-exponent 0. On the other hand, again by Lemma 2, $\chi'(C_{\lambda^\sigma})$ is even, since $\mu \neq \lambda$, and we conclude that (12) also has positive 2-exponent, as required. Thus, $A^{(k)}_{\chi\chi'} = 0$ for $\chi \neq \chi'$. Now suppose that $\chi = \chi' = \chi_\lambda$, say. We will show that (11) is odd in this case. Indeed, as before we see that all summands corresponding to conjugacy classes C with $C \neq C_{\lambda^\sigma}$ are rational numbers having positive 2-exponent. However, the term

$$\frac{|C_{\lambda^\sigma}|}{n!} \chi_\lambda^{2^k+1}(C_{\lambda^\sigma})$$

corresponding to $C = C_{\lambda^\sigma}$ is a rational number with 2-exponent 0. Hence, we have found that $A^{(k)} = I$ (the identity matrix) for all k with $2^k > n$. In order to obtain

information on $\mathcal{M}$ itself, we take k large enough to ensure that $2^k > n$, and compute $A^{(k+1)}$ by using the block structure of $\mathcal{M}$ and $\mathcal{M}^k$, together with the fact that $A^{(k)} = I$. We find that

$$A^{(k+1)}_{\chi\chi'} = \sum_{\chi''} A^{(k)}_{\chi\chi''} A^{(1)}_{\chi''\chi'} + 2 \sum_{\chi''} B^{(k)}_{\chi\chi''} C^{(1)}_{\chi''\chi'} = A^{(1)}_{\chi\chi'}.$$

Hence, $I = A^{(k+1)} = A^{(1)}$, which gives (ii). □

6. The main lemma and proof of Theorem 3

6.1. **The main lemma.** Call an irreducible character χ of S_n a 2-*core* character, if $\frac{n!}{\chi(1)}$ is odd. Note that, since the degree of an irreducible representation of a finite group G always divides $|G/\zeta_1(G)|$, this concept is well defined for arbitrary finite groups; cf. [13] or [12, Chap. V, Satz 17.10]. For $G = S_n$, the hook formula shows that an irreducible character χ_λ is 2-core if and only if all hook lengths of the associated partition λ are odd. The latter condition is easily seen to be equivalent to requiring that λ is of the form $\triangle = (k, k-1, \ldots, 1)$ for some $k \geq 1$. It follows that S_n has a 2-core character if and only if $n = \frac{k(k+1)}{2}$ is a triangular number, in which case $\chi_\triangle$ is the unique 2-core character; in particular, the 2-core character is symmetric. With these preliminaries, we are now in a position to establish the following result, which is the decisive tool in proving Theorem 3.

Lemma 4. *Let $w \in \mathcal{W}_2$ be a word involving d generators, and let χ be an irreducible character of S_n.*

(i) *If $d \geq 2$, then $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is an integer.*

(ii) *If $d \geq 3$ and χ is not 2-core, then $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is even.*

(iii) *If $d \geq 2$, χ is 2-core and $w \in \mathcal{W}_1$, then $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is odd.*

Proof. Let χ be an irreducible character of S_n. Using Lemma 1, we see by induction on d that $(\chi(1))^{d-1}\alpha_\chi(w)$ is integral for $d \geq 1$ and all $w \in \mathcal{W}_2$, implying (i). Moreover, if χ is not 2-core, then $\frac{n!}{\chi(1)}$ is even, hence, for $d \geq 3$, $(n!)^{d-2}\chi(1)\alpha_\chi(w)$ is even, as required in (ii). Now suppose that $\chi = \chi_\triangle$ is 2-core, and that $w \in \mathcal{W}_1$. We want to show that in this case $(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w)$ is odd. This is done by induction on the formation length of words in $\mathcal{W}_1$. By Lemma 1 (i), our claim holds for $w = x_i^2$ and $w = [x_i, x_j]$. Assume that our claim is true for words $w_1, w_2 \in \mathcal{W}_1$ having no generator in common, let d_i be the number of generators involved in w_i, and consider the word $w = w_1 w_2$. Then w involves $d = d_1 + d_2$ generators, and by part (ii) of Lemma 1,

$$(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w) = (\chi_\triangle(1))^{d_1-1}\alpha_{\chi_\triangle}(w_1) \cdot (\chi_\triangle(1))^{d_2-1}\alpha_{\chi_\triangle}(w_2),$$

which is odd, since by assumption both factors $(\chi_\triangle(1))^{d_i-1}\alpha_{\chi_\triangle}(w_i)$ are odd. Thus, it remains to show that our claim holds for $w = [v, x_i]$, provided it is correct for $v \in \mathcal{W}_1$ and x_i does not occur in v. By Lemma 1 (iii),

$$(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w) = (\chi_\triangle(1))^{d-2} \sum_{\chi'} \alpha_{\chi'}(v)\langle \chi_\triangle^2 \mid \chi' \rangle.$$

Now we distinguish the cases $d \geq 3$ and $d = 2$. If $d \geq 3$ and χ' is not 2-core, then $(\chi'(1))^{d-2}\alpha_{\chi'}(v)$ is integral, and $\chi_\triangle(1)$ is divisible by a higher power of 2 than $\chi'(1)$. Hence, the terms in the last sum not coming from the 2-core character $\chi_\triangle$ sum to an even integer, and we have

$$(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w) \equiv (\chi_\triangle(1))^{d-2}\alpha_{\chi_\triangle}(v)\langle \chi_\triangle^2 \mid \chi_\triangle\rangle \mod 2.$$

By assumption, $(\chi_\triangle(1))^{d-2}\alpha_{\chi_\triangle}(v)$ is odd, as is the multiplicity $\langle \chi_\triangle^2 \mid \chi_\triangle\rangle$ by Lemma 3 (ii). Hence, $(\chi_\triangle(1))^{d-1}\alpha_{\chi_\triangle}(w)$ is odd, and the induction on formation length is complete in this case. Now suppose that $d = 2$. Then $w = [x_i^2, x_j]$ for some $i \neq j$, and by Lemma 1 (iii),

$$\chi_\triangle(1)\alpha_{\chi_\triangle}(w) = \sum_{\chi'} \langle \chi_\triangle^2 \mid \chi'\rangle.$$

By Lemma 3 (i) for $k = 1$, the right-hand side is congruent modulo 2 to

$$\sum_{\substack{\lambda\vdash n\\ \lambda=\lambda'}} \langle \chi_\triangle^2 \mid \chi_\lambda\rangle,$$

which is odd by part (ii) of this lemma. □

6.2. **Proof of Theorem 3.** Let $w \in \mathcal{W}_2$ be a word involving $d \geq 3$ generators. By the exponential principle, the subgroup numbers $s_n(\Gamma_w)$ are related to the sequence $h_n(\Gamma_w) = |\mathrm{Hom}(\Gamma_w), S_n)|/n!$ via the equation[2]

$$nh_n(\Gamma_w) = \sum_{\nu=0}^{n-1} s_{n-\nu}(\Gamma_w)h_\nu(\Gamma_w), \quad n \geq 1.$$

Also, since homomorphisms of Γ_w to S_n can be identified with solutions of the equation $w(x_1, \ldots, x_d) = 1$ in S_n, we have

$$h_n(\Gamma_w) = (n!)^{d-2} \sum_{\chi\in\mathrm{Irr}(S_n)} \alpha_\chi(w)\chi(1).$$

From Lemma 4 we know that, for $w \in \mathcal{W}_1$, $h_n(\Gamma_w)$ is odd if and only if n is a triangular number, and that, if $w \in \mathcal{W}_2$, the condition that n be triangular is still necessary for $h_n(\Gamma_w)$ to be odd. Hence, for $n \geq 1$, we find that modulo 2

$$\begin{aligned} s_n(\Gamma_w) &= nh_n(\Gamma_w) \; - \sum_{\nu=1}^{n-1} s_{n-\nu}(\Gamma_w)h_\nu(\Gamma_w) \\ &\equiv \sum_{\substack{k\geq 1\\ k(k+1)<2n}} \alpha_k s_{n-k(k+1)/2}(\Gamma_w) \; + \; \delta(n), \end{aligned}$$

where $\alpha_1 = 1$, and $\alpha_k = 1$ for all k if $w \in \mathcal{W}_1$, the correction term $\delta(n)$ coming from the term $nh_n(\Gamma_w)$.

[2]Cf. for instance [3, Prop. 1].

References

[1] C. Curtis and I. Reiner, *Methods of Representation Theory*, Wiley Interscience, New York, 1981.

[2] H. Davenport, *The Higher Arithmetic*, sixth edition, Cambridge University Press, 1992.

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

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

[5] M. du Sautoy and F. Grunewald, Analytic properties of zeta functions and subgroup growth, *Annals of Math.*, to appear.

[6] C. F. Gauss, *Disquisitiones Arithmeticae* (Lipsia in commissis apud Gerh. Fleischer Iun), 1801; English translation by A. Clarke (New York: Springer-Verlag), 1986.

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

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

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

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

[11] E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, Academische Verlagsgesellschaft, Leipzig, 1923; reprinted (New York: Chelsea Publishing Company) 1970. English translation by G. Brauer and J. Goldman with R. Kotzen as *Lectures on the Theory of Algebraic Numbers* (New York: Springer-Verlag), 1981.

[12] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1979.

[13] N. Ito, On the degrees of irreducible representations of a finite group, *Nagoya Math. J.* **3** (1951), 5 – 6.

[14] A. Kerber, *Algebraic Combinatorics via Finite Group Actions*, BI–Wiss.–Verl., Mannheim, 1991.

[15] A.-M. Legendre, *Essai sur la Théorie des Nombres*, Paris, 1798. Fourth edition as *Théorie des Nombres*, 1830; reprinted (Paris: Albert Blanchard) 1955.

[16] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications Vol. 20, Cambridge University Press, 1997.

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

[18] A. Lubotzky, Counting finite index subgroups. In: Groups '93 Galway/St Andrews, LMS Lecture Notes Series No. 212, Cambridge University Press, 1995, 368 – 404.

[19] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), 267 – 295.

[20] A. Lubotzky, A. Mann, and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.* **82** (1993), 363 – 371.

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

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

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

[24] T. Müller, Parity patterns in Hecke groups and Fermat primes, to appear in *Proc. 1999 Bielefeld Conference on Geometric and Combinatorial Group Theory* (H. Helling and T.W. Müller editors)

[25] T. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, to appear in *Bull. London Math. Society.*

[26] T. Müller, Modular subgroup arithmetic in free products, submitted.

[27] T. Müller, Modular subgroup arithmetic – the state of the art. To appear in: Proc. 2001 Durham Symposium on Groups, Geometries, and Combinatorics.

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

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

[30] T. Müller and J.–C. Puchta, Character theory of symmetric groups and subgroup growth of surface groups, *J. London Math. Society*, to appear.

[31] T. Scharf, Die Wurzelanzahlfunktion in symmetrischen Gruppen, *J. Algebra* **139** (1991), 446 – 457.

Thomas W. Müller, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, England
E-mail: T.W.Muller@qmul.ac.uk

Jan–Christoph Puchta, Mathematical Institute, University of Oxford, 24 – 29 St Giles', Oxford OX1 3LB, England
E-mail: puchta@maths.ox.ac.uk