PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 134, Number 4, Pages 1003–1012
S 0002-9939(05)08074-3
Article electronically published on October 5, 2005

DISCRETE LOGARITHMS IN FREE GROUPS

YIANNIS N. PETRIDIS AND MORTEN S. RISAGER

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. For the free group on n generators we prove that the discrete logarithm is distributed according to the standard Gaussian when the logarithm is renormalized appropriately.

1. INTRODUCTION

Let $\Gamma = F(A_1, \dots, A_n)$, $n \geq 2$, be the free group on n generators. We define additive homomorphisms on the generators

$$\begin{array}{rccc} \log_j : & \Gamma & \to & \mathbb{Z} \\ & A_i & \mapsto & \delta_{ij}. \end{array} \tag{1.1}$$

Hence $\log_j$ counts the number of occurrences (with signs) of the generator A_j. We want to study the distribution of this discrete logarithm as the word length grows to infinity. Our main result is that, after a suitable re-normalization and restriction, the discrete logarithm is distributed according to a standard Gaussian distribution. More precisely, let

$$\mathfrak{log}_j(\gamma) = \sqrt{\frac{n-1}{\mathrm{wl}\,(\gamma)}}\log_j(\gamma). \tag{1.2}$$

Here $\mathrm{wl}\,(\gamma)$ denotes the word length of $\gamma \in \Gamma$. Let Γ_c be the set of cyclically reduced words in Γ.

Theorem 1.1. *In Γ_c the function $\mathfrak{log}_j$ has asymptotically a standard Gaussian distribution. More precisely*

$$\frac{\#\{\gamma \in \Gamma_c | \,\mathrm{wl}\,(\gamma) \leq l,\, \mathfrak{log}_j(\gamma) \in [a,b]\}}{\#\{\gamma \in \Gamma_c | \,\mathrm{wl}\,(\gamma) \leq l\}} \to \frac{1}{\sqrt{2\pi}}\int_a^b \exp\left(-\frac{x^2}{2}\right) dx \text{ as } l \to \infty.$$

After proving this theorem we discovered that I. Rivin arrived at a similar theorem in [10, Theorem 5.1] (see also [12]). Rivin's proof uses certain results on Chebyshev polynomials. Our proof uses character perturbations of the adjacency operator of a singleton graph (see Figure 1 where $n = 4$).

There is a fundamental identity, due to Ihara, which relates geometric entities (lengths of closed paths on the graph) to the spectrum of the adjacency operator of the graph. We consider this identity when the system transforms according

Received by the editors August 9, 2004 and, in revised form, November 12, 2004.
2000 *Mathematics Subject Classification.* Primary 05C25; Secondary 11M36.
The first author was partially supported by PSC CUNY Research Award, No. 60007-33-34, and NSF grant DMS 0401318.

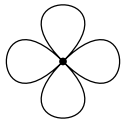

FIGURE 1.

to a certain smooth family of characters related to the discrete logarithms. By differentiating in the character family we can extract enough information about the relevant generating functions to calculate the moments of the random variable in Theorem 1.1. Apart from the use of this identity our proof is elementary. Our method is very powerful and has been used by the authors in a series of papers [6, 7, 9, 8] to prove distribution results of additive homomorphisms in various different contexts. In fact we were motivated by our previous results to investigate the normal distribution on the level of the group without considering its action as isometries on hyperbolic space.

2. From free groups to graphs

Let $\Gamma = F(A_1, \dots, A_n)$, $n \geq 2$, be the free group on n generators. We want to relate a finite graph to Γ. We refer to [11, 13, 4, 3] for the basics on graphs and further explanation of some of the terminology that we use. We mostly follow the terminology of [3].

Every $g \in \Gamma$ is uniquely represented by a reduced word, i.e.

$$\gamma = \prod_{i=1}^{k} A_{m_i}^{\epsilon_i}, \qquad m_i \in \{1, \dots, n\}, \epsilon_i \in \{\pm 1\},$$

in which there does not exist i_0 such that $m_{i_0} = m_{i_0+1}$ and $\epsilon_{i_0}\epsilon_{i_0+1} = -1$. Hence

$$\log_j(\gamma) = \sum_{\substack{i=1 \\ m_i = j}}^{k} \epsilon_{m_i} \tag{2.1}$$

counts (with signs) the number of occurrences of A_j in the reduced word representation of γ. We define the word length of γ to be $\mathrm{wl}\,(\gamma) = k$. We also define $g \in \Gamma$ to be cyclically reduced if

$$\gamma \circ \gamma = \prod_{i=1}^{k} A_{m_i}^{\epsilon_i} \prod_{i=1}^{k} A_{m_i}^{\epsilon_i}$$

is reduced (or equivalently if either $\epsilon_1\epsilon_k \neq -1$ or $m_1 \neq m_k$). We consider the set Γ_c of cyclically reduced words

$$\Gamma_c = \{\gamma \in \Gamma | \gamma \text{ is cyclically reduced}\}.$$

There is an infinite-to-one map ψ (cyclic reduction) from Γ to Γ_c, and this map satisfies $\log_j(\gamma) = \log_j(\psi(\gamma))$.

Let $S = \{A_1, \dots, A_n\}$ and consider the $2n$-regular Cayley graph $X = X(\Gamma, S)$, i.e. the graph having vertices Γ and (positive) edges $\Gamma \times S$ where the edge $(g, s) \in \Gamma \times S$ has the following origin and terminus:

$$o(g, s) = g, \qquad t(g, s) = gs.$$

The group Γ acts (strictly hyperbolic) by isometric isomorphisms on X, and the quotient graph $\Gamma\backslash X$ is $2n$-regular and has one vertex.

We denote by $\mathrm{C}^{\mathrm{red}}$ the set of closed reduced paths on the graph. The set of elements in $\mathrm{C}^{\mathrm{red}}$ of length n is denoted by $\mathrm{C}_n^{\mathrm{red}}$. For this particular graph the following is easy to verify:

Lemma 2.1. *There is a one-to-one correspondence between* $\mathrm{C}_m^{\mathrm{red}}$ *and the set of cyclically reduced group elements* $\gamma \in \Gamma_c$ *with* $\mathrm{wl}\,(\gamma) = m$.

We can now therefore define an additive homomorphism $\widetilde{\log}_j$ on $\mathrm{C}^{\mathrm{red}}$ by fixing an isomorphism $\phi : \mathrm{C}_1^{\mathrm{red}} \to \{\gamma \in \Gamma_c | \,\mathrm{wl}\,(\gamma) = 1\}$ and defining $\widetilde{\log}_j(C) = \log_j(\phi(C))$. By an obvious abuse of notation we shall often write $\log_j(C)$ instead of $\widetilde{\log}_j(C)$.

3. The Ihara zeta function

We now briefly explain the basics of the Ihara zeta function. There is a close resemblance between the Ihara zeta function and the Selberg zeta function [1]. We refer to [13, 4, 3] for further details. Let X be a $(q+1)$-regular infinite tree ($q \geq 2$) and let Γ be a strictly hyperbolic free subgroup of isometric automorphisms of X with finite $(q+1)$-regular quotient graph

$$\#\,\mathrm{vert}\,(\Gamma\backslash X) < \infty. \tag{3.1}$$

Furthermore let $\chi : \Gamma \to S^1$ be a unitary character. Consider

$$L^2(X,\chi) = \{f : \mathrm{vert}\,(X) \to \mathbb{C}\,|f(\gamma v) = \chi(\gamma) f(v) \text{ for all } \gamma \in \Gamma, v \in \mathrm{vert}\,(X)\,\}$$

together with the inner product

$$\langle f, g\rangle = \sum_{v \in \mathrm{vert}(\Gamma\backslash X)} f(v)\overline{g(v)}.$$

We note that this is a finite-dimensional Hilbert space of dimension $\dim L^2(X,\chi) = \#\,\mathrm{vert}\,(\Gamma\backslash X)$. We consider the adjacency operator $A(\Gamma,\chi) : L^2(X,\chi) \to L^2(X,\chi)$ defined by

$$(A(\Gamma,\chi)f)(v) = \sum_{v' \sim v} f(v'). \tag{3.2}$$

Here $v' \sim v$ means that v' is adjacent to v. The adjacency operator is self-adjoint with spectrum contained in $[-(q+1), q+1]$.

Let $\mathfrak{P}_\Gamma$ be the set of primitive conjugacy classes in Γ different from the unit class. For $\{P\} \in \mathfrak{P}_\Gamma$ we define the degree

$$\deg(P) = \min_{v \in \mathrm{vert}(X)} l(v, Pv) \tag{3.3}$$

where $l(v,v')$ is the length of the geodesic from v to v'.

The Ihara zeta function is defined, for $u \in \mathbb{C}$ with $|u| < q^{-1}$, by

$$Z(\Gamma,\chi;u) = \prod_{\{P\} \in \mathfrak{P}_\Gamma} (1 - \chi(P) u^{\deg P})^{-1}. \tag{3.4}$$

There is a fundamental identity, due to Ihara, which relates this geometric object to the spectrum of the adjacency operator. More precisely, we have the following explicit determinant representation of the Ihara zeta function [4].

Theorem 3.1 (Ihara)**.**

$$Z(\Gamma,\chi;u)=(1-u^2)^{-g}\det\left(1-uA(\Gamma,\chi)+qu^2\right)^{-1}, \tag{3.5}$$

where $g=(q-1)\#\operatorname{vert}(\Gamma\backslash X)/2$.

This gives immediately that the Ihara zeta function admits meromorphic continuation to the whole complex plane. We consider the logarithmic derivative of $Z(\Gamma,\chi;u)$ and find

$$\begin{aligned} u\frac{d}{du}\log Z(\Gamma,\chi;u) &= u\sum_{\{P\}\in\mathfrak{P}_\Gamma}\frac{\chi(P)\deg P u^{\deg P-1}}{1-\chi(P)u^{\deg P}} \\ &= \sum_{n=1}^{\infty}\sum_{\{P\}\in\mathfrak{P}_\Gamma}\chi(P^n)\deg P u^{n\deg P} \\ &= \sum_{m=1}^{\infty}n_{\Gamma,\chi}(m)u^m, \end{aligned} \tag{3.6}$$

where

$$n_{\Gamma,\chi}(m)=\sum_{\substack{n\deg P=m\\ n\in\mathbb{N},\{P\}\in\mathfrak{P}_\Gamma}}\chi(P^n)\deg P. \tag{3.7}$$

There is a one-to-one correspondence between primitive conjugacy classes of Γ of degree d, $\mathfrak{P}_\Gamma(d)$ and primitive cycles in $\Gamma\backslash X$ of length d, $\operatorname{Prim}_{\Gamma\backslash X}(d)$. The natural map from the set of closed reduced prime paths of length d in $\Gamma\backslash X$, $\mathrm{C}_d^{\mathrm{red,prime}}$, to the set of primitive cycles of length d in $\Gamma\backslash X$ is d-to-one (each of the d vertices can be a starting point for the cycle). We therefore have

$$n_{\Gamma,\chi}(m)=\sum_{d|m}d\sum_{\{P\}\in\mathfrak{P}_\Gamma}\chi(P^{m/d})=\sum_{d|m}\sum_{C\in\mathrm{C}_d^{\mathrm{red,prime}}}\chi(C^{m/d})=\sum_{C\in\mathrm{C}_m^{\mathrm{red}}}\chi(C).$$

Using (3.5) we get

$$\sum_{m=1}^{\infty}n_{\Gamma,\chi}(m)u^m=\frac{2gu^2}{1-u^2}-u\frac{\frac{d}{du}\det(1-uA(\Gamma,\chi)+qu^2)}{\det(1-uA(\Gamma,\chi)+qu^2)}. \tag{3.8}$$

When $\chi=1$ the adjacency operator has $q+1$ as an eigenvalue with the identity as eigenfunction. Hence, in this case, we see that (3.8) has a pole at $u=q^{-1}$.

4. Generating functions

We now explain how to use the Ihara zeta function to get information about the generating functions relevant to Theorem 1.1. Since we are ultimately interested in the case of the singleton graph constructed in section 2 we assume for simplicity that the quotient in the previous section has only one vertex. In the case of the graph from section 2 we have $q+1=2n$.

We define a family of unitary characters on Γ by

$$\chi_\epsilon(\gamma)=\exp(i\epsilon\log_j(\gamma)).$$

In this simple situation the adjacency operator is simply a multiplication operator:

$$(A(\Gamma,\chi_\epsilon)f)(v)=\sum_{i=1}^{n}(\chi_\epsilon(A_i)+\chi_\epsilon(A_i)^{-1})f(v). \tag{4.1}$$

For simplicity we let

$$A(\epsilon) = \sum_{i=1}^{n} (\chi_\epsilon(A_i) + \chi_\epsilon(A_i)^{-1}) = 2(n-1) + 2\cos(\epsilon). \tag{4.2}$$

Equation (3.8) now takes the form

$$\sum_{m=1}^{\infty} n_{\Gamma,\chi_\epsilon}(m) u^m = \frac{2gu^2}{1-u^2} + \frac{uA(\epsilon) - 2qu^2}{1 - uA(\epsilon) + qu^2}. \tag{4.3}$$

We denote the left-hand side by $G(u,\epsilon)$. This is the generating function relevant to the problem we are studying. When $\epsilon = 0$ this function has a simple pole at $u = q^{-1}$ with residue

$$\operatorname{res}_{u=q^{-1}} G(u,0) = -q^{-1}. \tag{4.4}$$

We wish to understand

$$G^{(k)}(u) := \frac{d^k}{d\epsilon^k} G(u,\epsilon)\bigg|_{\epsilon=0} = \sum_{m=1}^{\infty} \left(\sum_{C \in \mathrm{C}_m^{\mathrm{red}}} i^k \log_j(C)^k \right) u^m. \tag{4.5}$$

The convergence is uniform in ϵ, by comparison with the series with $\epsilon = 0$, so we can differentiate termwise.

From (4.3) we get immediately the following result:

Theorem 4.1. *The function $G^{(k)}(u)$ admits meromorphic continuation to the whole complex plane. The points $u = q^{-1}$, $u = 1$ are the only possible poles when $n \geq 1$. The function $G(u) = G^{(0)}(u)$ has poles at $u = \pm 1$ and $u = q^{-1}$.*

We now calculate the pole order and leading term of the pole at $u = q^{-1}$. When $k \geq 1$, Eq. (4.3) gives

$$G^{(k)}(u) = \sum_{l=0}^{k} \binom{k}{l} (uA^{(l)}(0) - \delta_{l=0} 2qu^2) \, \frac{d^{k-l}}{d\epsilon^{k-l}} (1 - uA(\epsilon) + qu^2)^{-1}\bigg|_{\epsilon=0}. \tag{4.6}$$

Clearly we have

$$A^{(l)}(0) = \begin{cases} 2n, & \text{if } l = 0, \\ 0, & \text{if } l \text{ is odd}, \\ 2(-1)^{l/2}, & \text{if } l \geq 2 \text{ is even}. \end{cases} \tag{4.7}$$

We first analyze the leading term L_l of

$$\frac{d^l}{d\epsilon^l} (1 - uA(\epsilon) + qu^2)^{-1}\bigg|_{\epsilon=0}. \tag{4.8}$$

Since

$$(1 - uA(\epsilon) + qu^2)(1 - uA(\epsilon) + qu^2)^{-1} = 1, \tag{4.9}$$

we find that (4.8) equals

$$(1 - uA(0) + qu^2)^{-1} \sum_{r=0}^{l-1} \binom{l}{r} A^{(l-r)}(0) u \, \frac{d^r}{d\epsilon^r} (1 - uA(\epsilon) + qu^2)^{-1}\bigg|_{\epsilon=0}. \tag{4.10}$$

When $l = 1$ it is obvious from (4.7) that this vanishes. By induction and (4.7) we conclude that

$$\frac{d^l}{d\epsilon^l}(1 - uA(\epsilon) + qu^2)^{-1}\Big|_{\epsilon=0} = 0 \tag{4.11}$$

when l is odd. Alternatively $1 - uA(\epsilon) + qu^2$ is an even function.

From (4.10), (4.11), and (4.7) an easy induction argument now shows that when l is even (4.8) has a pole of order $l/2 + 1$ and the leading term L_l satisfies the recurrence relation

$$L_l = (\mathrm{res}_{u=q^{-1}}(1 - A(0)u + qu^2)^{-1})\binom{l}{l-2}A^{(2)}(0)q^{-1}L_{l-2}. \tag{4.12}$$

It follows easily that

$$L_l = -\frac{1}{q^{l/2}}\frac{l!}{(q-1)^{l/2+1}}. \tag{4.13}$$

Therefore, the main term in $G^{(k)}(u)$, see (4.6), comes from $l = 0$, and using (4.13) we get the following theorem:

Theorem 4.2. *When k is odd the function $G^{(k)}(u)$ is identically zero. When k is even $G^{(k)}(u)$ has a pole at $u = q^{-1}$ of order $k/2 + 1$ and the leading term in the Laurent expansion around $u = q^{-1}$ equals*

$$-\frac{k!}{q^{k/2+1}(q-1)^{k/2}}.$$

We notice that the vanishing of $G^{(k)}(u)$ for k odd is also clear from the fact that

$$\sum_{C \in \mathrm{C}_m^{\mathrm{red}}} \log_j(C)^k = 0.$$

This fact is clear since if C is a reduced path of length m, then the inverse path is also a reduced path of length m and $\log_j(C)^k + \log_j(C^{-1})^k = 0$ when m is odd.

5. Summations

In this section we want to find asymptotics as $T \to \infty$ of the following sums:

$$\sum_{\substack{\gamma \in \Gamma_c \\ \mathrm{wl}(\gamma) \leq T}} \log_j(\gamma)^k. \tag{5.1}$$

In principle we can find exact expressions for these sums. We show how this is done when $k = 0$. In the general situation we settle with asymptotics since this is all we need for Theorem 1.1. We do this on the basis of the calculations of the previous chapter and a Tauberian theorem to be proved below. We notice that from Lemma 2.1 and the fact that if $\phi(C) = \gamma$, then $l(C) = \mathrm{wl}\,(\gamma)$ we have that (5.1) equals

$$\sum_{m \leq T} \sum_{C \in \mathrm{C}_m^{\mathrm{red}}} \log_j(C)^k. \tag{5.2}$$

For k odd the discussion at the end of the last section shows that (5.1) is identically zero.

We have

$$\frac{1}{1 - u2n + qu^2} = \frac{1}{q-1}\left(\frac{q}{1-qu} - \frac{1}{1-u}\right).$$

From this we see, using a geometric expansion, that

$$\frac{u2n - 2qu^2}{1 - u2n + qu^2} = \sum_{m=1}^{\infty} (q^m + 1)u^m.$$

Since

$$\frac{2gu^2}{1-u^2} = \frac{q-1}{2} \sum_{m=1}^{\infty} \left(1 + (-1)^m\right) u^m,$$

we conclude that

$$G^{(0)}(u) = \sum_{m=1}^{\infty} \#\,\mathrm{C}_m^{\mathrm{red}}\, u^m = \sum_{m=1}^{\infty} \left(q^m + 1 + \frac{q-1}{2} \left(1 + (-1)^m\right) \right) u^m$$

when $|u| < q^{-1}$. Using Lemma 2.1 and the uniqueness of Taylor expansions, we proved the following theorem:

Theorem 5.1. *Let Γ be the free group on n elements and Γ_c the set of cyclically reduced words in Γ. Then the number of cyclically reduced words of word length m equals*

$$\#\{\gamma \in \Gamma_c | \operatorname{wl}(\gamma) = m\} = (2n-1)^m + 1 + (n-1)\left(1 + (-1)^m\right).$$

We notice that this is [10, Theorem 1.1]. In principle we can use the same technique as above for any k using (4.6). This would give explicit, though quite complicated, expressions for

$$\sum_{C \in \mathrm{C}_m^{\mathrm{red}}} \log_j(C)^k.$$

For simplicity we use only the fact that we have calculated the leading term of (4.6) to obtain the main term and sharp error estimates for (5.2). To do this we need the following proposition:

Proposition 5.2. *Assume that*

$$f(u) = \sum_{m=0}^{\infty} c_m u^m$$

has radius of convergence $R = q^{-1} \leq 1$. Assume further that

(i) *f admits meromorphic continuation to an open set containing the closed unit disc in $\mathbb{C}$;*
(ii) *the points $u = q^{-1}$ and $u = 1$ are the only possible poles in the closed unit disc;*
(iii) *the pole at q^{-1} is of order k with leading term $a_k(u - q^{-1})^{-k}$.*

Then

$$\sum_{m=0}^{l} c_m = \frac{(-q)^k a_k}{(q-1)(k-1)!} q^{l+1} l^{k-1} + O(q^{l+1} l^{k-2}).$$

To prove this proposition we need the following elementary lemma. We shall write $(k)_m = k(k+1)\cdots(k=(m-1))$.

Lemma 5.3. *Let $q > 1$ and $k \in \mathbb{N}$. Then*

$$\sum_{m=0}^{l} \frac{(k)_m}{m!} = \frac{1}{k!} l^k + O(l^{k-1}), \tag{5.3}$$

$$\sum_{m=0}^{l} \frac{(k)_m}{m!} q^m = \frac{1}{(q-1)(k-1)!} q^{l+1} l^{k-1} + \begin{cases} O(q^{l+1} l^{k-2}), & \text{if } k \geq 2, \\ O(1) & \text{if } k = 1. \end{cases} \tag{5.4}$$

Proof. To prove (5.3) we notice that $(k)_m/m! = (m+1)(m+2)\cdots(m+k-1)/(k-1)!$. Using the elementary estimate

$$\sum_{m=0}^{l} m^{k-1} = \frac{1}{k} l^k + O(l^{k-1})$$

proves the claim.

To prove (5.4) we define

$$a(k,m,q) = \frac{(k)_m}{m!} q^m \quad \text{and} \quad A(k,l,q) = \sum_{m=0}^{l} a(k,m,q).$$

Then using $a(k,m,q) = (k+m-1)a(k-1,m,q)/(k-1)$ (when $k \neq 1$) and partial summation we find

$$\begin{aligned} A(k,l,q) &= \frac{1}{k-1} \sum_{m=0}^{l} a(k-1,m,q)(k+m-1) \\ &= \frac{1}{k-1} A(k-1,l,q)(k+l-1) - \frac{1}{k-1} \int_0^l A(k-1,t,q)dt \\ &= \frac{l}{k-1} A(k-1,l,q) + A(k-1,l,q) - \frac{1}{k-1} \int_0^l A(k-1,t,q)dt. \end{aligned} \tag{5.5}$$

When $k = 1$ the claim is obvious since in this case $(k)_m/m! = 1$. The remaining cases now follow from (5.5) by induction. □

To prove Proposition 5.2 we let

$$\sum_{j=1}^{k} \frac{a_j}{(u-q^{-1})^j}, \quad \text{resp.} \quad \sum_{j=1}^{k'} \frac{b_j}{(u-1)^j},$$

be the singular parts of f at $u = q^{-1}$, resp. $u = 1$. Now the function

$$f(u) - \sum_{j=1}^{k} \frac{a_j}{(u-q^{-1})^j} - \sum_{j=1}^{k'} \frac{b_j}{(u-1)^j} \tag{5.6}$$

is regular in an open disc containing the closure of the unit disc. Using the series expansions

$$\begin{aligned} \frac{1}{(u-1)^j} &= (-1)^j \sum_{m=0}^{\infty} \frac{(j)_m}{m!} u^m, \\ \frac{1}{(u-q^{-1})^j} &= q^j (-1)^j \sum_{m=0}^{\infty} \frac{(j)_m q^m}{m!} u^m, \end{aligned}$$

we conclude that the series

$$\sum_{m=0}^{\infty}\left(c_m-\sum_{j=1}^{k}a_j(-q)^j\frac{(j)_m}{m!}q^m-\sum_{j=1}^{k'}b_j(-1)^j\frac{(j)_m}{m!}\right)u^m$$

has radius of convergence strictly larger than 1. In particular it is convergent at $u=1$, that is

$$\sum_{m=0}^{l}c_m=\sum_{m=0}^{l}\sum_{j=1}^{k}a_j(-q)^j\frac{(j)_m}{m!}q^m+\sum_{m=0}^{l}\sum_{j=1}^{k'}b_j(-1)^j\frac{(j)_m}{m!}+o(1) \tag{5.7}$$

as $l\to\infty$.

It follows now from Lemma 5.3 that

$$\sum_{m=0}^{l}c_m=\frac{(-q)^k a_k}{(q-1)(k-1)!}q^{l+1}l^{k-1}+O(q^{l+1}l^{k-2}), \tag{5.8}$$

which finishes the proof of the proposition.

We notice that we have proved a Wiener-Ikehara-type Tauberian theorem (see [2]) for power series with *general* coefficients under the assumption that the sum admits meromorphic continuation to a disk containing the closure of the unit disc. Obviously the proposition can be easily generalized in many directions, but since we only need it in the generality stated we refer from doing so.

Using Proposition 5.2, Theorem 4.1, and Theorem 4.2 we get

Theorem 5.4.

$$\sum_{m=0}^{l}\sum_{C\in\mathrm{C}_m^{\mathrm{red}}}\log_j(C)^k=\begin{cases}0 & \text{if } k \text{ is odd,}\\ \frac{k!}{(k/2)!}\frac{1}{(q-1)^{k/2+1}}q^{l+1}l^{k/2}+O(q^{l+1}l^{k/2-1}) & \text{if } k \text{ is even.}\end{cases}$$

We now define the normalized discrete logarithms to be

$$\mathfrak{log}_j(C)=\sqrt{\frac{g}{l(C)}}\log_j(C).$$

Here $l(C)$ is the length of the cycle C. We then define the random variable X_l with probability measure

$$P(X_l\in[a,b])=\frac{\#\{C\in\mathrm{C}^{\mathrm{red}}\,|l(C)\le l,\,\mathfrak{log}_j(C)\in[a,b]\}}{\#\{C\in\mathrm{C}^{\mathrm{red}}\,|l(C)\le l\}}.$$

We then calculate the asymptotic moments of these random variables, i.e. we find the asymptotics of

$$M_k(X_l)=\frac{1}{\#\{C\in\mathrm{C}^{\mathrm{red}}\,|l(C)\le l\}}\sum_{\substack{C\in\mathrm{C}^{\mathrm{red}}\\ l(C)\le l}}\mathfrak{log}_j(C)^k.$$

From Theorem 5.4 we find, using partial summation, that as $l\to\infty$,

$$M_k(X_l)\to\begin{cases}0 & \text{if } k \text{ is odd,}\\ \dfrac{k!}{2^{k/2}(k/2)!} & \text{if } k \text{ is even.}\end{cases} \tag{5.9}$$

The left-hand side equals the moments of the standard Gaussian and from a classical result due to Fréchet and Shohat (see [5, 11.4.C]) we conclude that

$$P(X_l \in [a,b]) \to \frac{1}{\sqrt{2\pi}} \int_a^b \exp\left(-\frac{x^2}{2}\right) dx \text{ as } l \to \infty. \tag{5.10}$$

Using the identification in Lemma 2.1 and the fact that if $\phi(C) = \gamma$, then $l(C) = \mathrm{wl}(\gamma)$ we arrive at Theorem 1.1.

Acknowledgments

We would like to thank Alexei B. Venkov, Dorian Goldfeld and Søren Galatius for valuable comments and suggestions.

References

[1] D. Hejhal, The Selberg trace formula for PSL(2, R). Vol. 1. Lecture Notes in Mathematics, 1001. Springer-Verlag, Berlin, 1976, vi+516pp. MR0439755 (55:12641)
[2] J. Korevaar, A century of complex Tauberian theory. Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 4, 475–531 (electronic). MR1920279 (2003g:40004)
[3] A. M. Nikitin, The Ihara-Selberg zeta function of a finite graph and symbolic dynamics, Algebra i Analiz **13** (2001), no. 5, 134–149; translation in St. Petersburg Math. J. **13** (2002), no. 5, 809–820. MR1882866 (2003f:11137)
[4] A. M. Nikitin and A. B. Venkov, The Selberg trace formula, Ramanujan graphs and some problems in mathematical physics. (Russian), Algebra i Analiz **5** (1993), no. 3, 1–76; translation in St. Petersburg Math. J. **5** (1994), no. 3, 419–484. MR1239898 (94m:11066)
[5] M. Loève, *Probability theory. I*, Fourth edition, Springer, New York, 1977. MR0651017 (58:31324a)
[6] Y. N. Petridis, Spectral deformations and Eisenstein Series Associated with Modular Symbols. Internat. Math. Res. Notices **2002**, no. 19, 991–1006. MR1903327 (2003h:11057)
[7] Y. N. Petridis, M. S. Risager, Modular symbols have a normal distribution, Geom. Funct. Anal. **14** (2004), no. 5, 1013–1043. MR2105951
[8] Y. N. Petridis, M. S. Risager, The distribution of values of the Poincaré pairing for hyperbolic Riemann surfaces, J. Reine Ang. Mat. **579** (2005), 159–173.
[9] M. S. Risager, On the distribution of modular symbols for compact surfaces, Internat. Math. Res. Notices **2004**, No. 41, 2125–2146. MR2078851
[10] I. Rivin, Growth in free groups (and other stories), arXiv:math.CO/9911076.
[11] J.-P. Serre, *Trees*, Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation, Springer, Berlin, 2003. MR1954121 (2003m:20032)
[12] R. Sharp, Local limit theorems for free groups, J. Math. Ann. **321** (2001), 4, p. 889–904. MR1872533 (2002k:20039)
[13] A. Terras, *Fourier analysis on finite groups and applications*, Cambridge Univ. Press, Cambridge, 1999. MR1695775 (2000d:11003)

Department of Mathematics and Computer Science, City University of New York, Lehman College, 250 Bedford Park Boulevard, West Bronx, New York 10468-1589
Current address: The Graduate Center, Mathematics Ph.D. Program, 365 Fifth Avenue, Room 4208 New York, New York 10016-4309
E-mail address: petridis@comet.lehman.cuny.edu

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade Building 530, 8000 Aarhus, Denmark
E-mail address: risager@imf.au.dk