ISRAEL JOURNAL OF MATHEMATICS 104 (1998), 129–144

STABLE MULTIPLICITIES IN THE LENGTH SPECTRUM OF RIEMANN SURFACES

BY

DAVID GINZBURG AND ZEÉV RUDNICK

Raymond and Beverley Sackler School of Mathematical Sciences, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: rudnick@math.tau.ac.il

ABSTRACT

Conjugacy classes in the free group on two generators which have the same trace for all two-dimensional representations form a trace class. The number of classes in a trace class is called the stable multiplicity of the trace class. We prove a condition for the stable multiplicity to be minimal, and suggest a necessary and sufficient condition.

1. Introduction

One of the most important invariants associated to a Riemann surface is the **length spectrum**: it is the set of lengths of the closed (unoriented) geodesics of the surface, including multiplicities (the metric is always taken to be of constant curvature $K = -1$). Unlike what happens for a generic metric of variable negative curvature, where all lengths have multiplicity one [1], it has been observed some time ago that in the constant curvature case, for any surface the multiplicities are **unbounded**. Our purpose in this note is to try to understand the reasons for this phenomenon.

The main reason for our interest lies in fine structure of the spectrum of the Laplacian on the surface: A few years ago it was discovered that the eigenvalues of the Laplacian appear to obey two distinct statistical laws depending on

Received March 20, 1996

the surface being arithmetic or not. In the generic non-arithmetic case numerical evidence and the heuristic arguments of M. Berry [3] suggest that the local statistics are GOE statistics. However, in the arithmetic case they appear to be Poissonian, as was first discovered numerically by physicists working in the field of "Quantum Chaos" [2], [4]. This was recently given some theoretical corroboration by work of Luo and Sarnak [10], who showed that the number variance of the spectrum of compact arithmetic surfaces was consistent with Poisson behavior, and by Bogomolny, Leyvraz and Schmit [5] who gave an argument for the pair correlation to be that of the Poisson distribution in the case of the modular surface.

One of the keys to understanding this anomaly (as already understood by Selberg several years ago [8]!) lies in the high multiplicity of lengths of closed geodesics for arithmetic surfaces. Recall that if we uniformize the surface as the quotient of the hyperbolic plane by a lattice $\Gamma \subset \mathrm{SL}(2,\mathbf{R})$, then the closed geodesics are parameterized by the (primitive, hyperbolic) conjugacy classes of Γ, and the length ℓ_γ of the closed geodesic corresponding to the conjugacy class $\{\gamma\}$ is given in terms of the trace of γ by $2\cosh(\ell_\gamma/2) = |\operatorname{tr}(\gamma)|$. The class of γ^{-1} corresponds to the same geodesic as γ but with reversed orientation. If we denote by $m(t)$ the number of conjugacy classes with trace t, then the Prime Geodesic Theorem asserts that $\sum_{t\le x} m(t) \sim x^2/\log(x^2)$. However, there is a dichotomy between the arithmetic and non-arithmetic cases: In the arithmetic case one has very high multiplicities (e.g. in the modular group the traces t range over integers so the number of possible values of the trace grows linearly* with x. This forces at least the mean multiplicity to be large, and in fact for the modular group one can show $m(t) \gg t^{1-\epsilon}$). In the non-arithmetic case the multiplicities are smaller, though their size is far from being understood.

That the multiplicities are unbounded even in the generic case was deduced by B. Randol [11] as a consequence of a construction of R. Horowitz [9] in the free group. To explain the connection, we look at the set of traces of elements of Γ. If we fix a set of generators $\gamma_1,\dots,\gamma_N$ of Γ, then the trace of any word $w(\gamma_1,\dots,\gamma_N)$ is a polynomial in the traces of the products $\operatorname{tr}(\gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_k})$, $1\le i_1<\dots<i_k\le n$. The polynomial depends only on the Γ-conjugacy class of w, and not on the embedding $\Gamma \hookrightarrow \mathrm{SL}(2,\mathbf{R})$. One defines the **trace class** of w

* The linear growth of the number of distinct traces is known to be a characterization of arithmetic groups, at least in the non-compact case, see Schmutz [12].

to be all elements w' of Γ such that $\operatorname{tr}\rho(w') = \operatorname{tr}\rho(w)$ for all two-dimensional complex representations $\rho : \Gamma \to \mathrm{SL}(2, \mathbf{C})$. The number of conjugacy classes in the trace class of w is called the **stable multiplicity** of the conjugacy class w. The stable multiplicities give a lower bound on the multiplicities of the length spectrum throughout the moduli space of Γ.

In this note we investigate stable multiplicities in the length spectrum by studying multiplicities of the trace classes in the free group on two generators $F_2 = \langle A, B\rangle$. Recall that given a surface group of genus $g \geq 2$ with canonical presentation

$$\Gamma_g = \langle a_1, b_1, \dots a_g, b_g : \prod_{i=1}^{g} a_i b_i a_i^{-1} b_i^{-1} = 1\rangle$$

we can embed $F_2 \hookrightarrow \Gamma_g$ by taking $A \mapsto a_1$, $B \mapsto a_2$, and it is a consequence of Dehn's solution of the word problem for surface groups [7], [13] that elements of F_2 are conjugate in F_2 if and only if they are conjugate in Γ_g.

Any conjugacy class has a representative $w_n(\mathbf{r}, \mathbf{m}) = A^{r_1} B^{m_1} \cdots A^{r_n} B^{m_n}$ with all $r_i, m_j \neq 0$ (other than in the case of the classes A^r, B^m), which is unique up to cyclic permutations:

$$A^{r_1} B^{m_1} \cdots A^{r_n} B^{m_n} \sim A^{r_2} B^{m_2} \cdots A^{r_n} B^{m_n} A^{r_1} B^{m_1} \sim \cdots$$

($\sim$ denoting conjugacy). Any trace class contains both w and its inverse w^{-1}, which are not conjugate if $w \neq 1$. Another member of the same trace class is gotten by "reading w backwards", that is, define

$$\theta(w(A, B)) := w(A^{-1}, B^{-1})^{-1} = B^{m_n} A^{r_n} \cdots B^{m_1} A^{r_1}.$$

It is easily seen that $\operatorname{tr}\theta(w) = \operatorname{tr} w$ (Lemma 2.1) and so the trace class of w contains the conjugacy classes of $w^{\pm 1}$ and $\theta(w)^{\pm 1}$. In case the trace class contains no other conjugacy classes, we will say that $\{w\}$ is **simple**.

By using the involution θ, one can construct examples of conjugacy classes which are not simple as follows: Given words $U = U(A, B)$, $V = V(A, B) \in F_2$, take any word $g = w(U, V)$, and set $h = w(U^{-1}, V^{-1})^{-1}$. The trace class of g will then contain the 8 conjugacy classes of $g^{\pm 1}$, $h^{\pm 1}$, $\theta(g)^{\pm 1}$ and $\theta(h)^{\pm 1}$. In this way each non-trivial decomposition of $w_n \in \langle A, B\rangle$ as $w_n = w_s(U, V)$ gives extra conjugacy classes in the same trace class (these are not always distinct, e.g. as in the case of $w = A^4$ which is a simple class). We believe that this is the only way to get non-simple trace classes (the examples of Horowitz [9] and Buser [6] are constructed in this fashion):

CONJECTURE 1: *If $w(A,B)$ admits no non-trivial decomposition as $w(A,B) = w'(U,V)$ then the trace class of w contains only the classes $w^{\pm 1}$ and $\theta(w)^{\pm 1}$.*

Our main result gives a sufficient condition for the class of $w_n(\mathbf{r},\mathbf{m})$ to be simple: We will say that $\mathbf{r} = (r_1,\dots,r_n) \in (\mathbf{Z}^\times)^n$ is **non-singular** if $r_k \neq \sum_{j\in S} r_j$ for all k and $S \subseteq \{1,\dots,n\}$, $S \neq \{k\}$. In particular, all the r_j are distinct, and $\sum_{j\in S} r_j \neq 0$ if S is non-empty.

THEOREM 1.1: *If $\mathbf{r}$, $\mathbf{m}$ are non-singular then the trace class of $w = w_n(\mathbf{r},\mathbf{m})$ contains only the conjugacy classes $\{w, w^{-1}, \theta(w), \theta(w)^{-1}\}$.*

The proof of Theorem 1.1 hinges on a formula for the first variation of $\operatorname{tr} w_n(\mathbf{r},\mathbf{m})$ as one moves from the boundary of the moduli space of representations. The point is that when $\rho : F_2 \to \mathrm{SL}(2,\mathbf{C})$ is **reducible**, then $\operatorname{tr} w_n(\mathbf{r},\mathbf{m})$ is easy to compute. In general, we will see that we may assume

$$\rho(A) = \begin{pmatrix} a & \\ & a^{-1}\end{pmatrix}, \quad \rho(B) = Z\begin{pmatrix} b & \\ & b^{-1}\end{pmatrix}Z^{-1} \quad \text{with } Z = \begin{pmatrix} 1 & x \\ 1 & x+1\end{pmatrix},$$

so that $x = 0$ are reducible representations. In Section 4 we give a relatively simple formula (Theorem 4.1) for the derivative d/dx of $\operatorname{tr} w_n$ at $x = 0$ which we use in Section 5 to prove Theorem 1.1.

2. A trace-preserving involution

Let $F_2 = \langle A, B\rangle$ be the free group on two generators; we think of A, B as matrices in $\mathrm{SL}(2,\mathbf{C})$. Every conjugacy class except classes of the identity, A^r and B^m, have a cyclically reduced representative of the form

$$w_n(\mathbf{r},\mathbf{m}) = A^{r_1}B^{m_1}\cdot\ldots\cdot A^{r_n}B^{m_n} \tag{2.1}$$

where all exponents are non-zero. We will call n the **syllable length** of the class. The representation (2.1) is unique up to simultaneous cyclic permutation of the indices $\mathbf{r}$, $\mathbf{m}$.

Let θ be the unique anti-involution of $F_2 = \langle A, B\rangle$ fixing the generators A, B: $\theta(w(A,B)) = w(A^{-1},B^{-1})^{-1}$, so that for $w_n = w_n(\mathbf{r},\mathbf{m})$ given by (2.1),

$$\theta(w_n) = B^{m_n}A^{r_n}B^{m_{n-1}}A^{r_{n-1}}\cdot\ldots\cdot B^{m_1}A^{r_1}.$$

Note that θ preserves conjugacy classes.

LEMMA 2.1: $\operatorname{tr} w_n = \operatorname{tr} \theta(w_n)$.

Proof: We first note that in the case that both A and B are **symmetric**, we have $\theta(w_n) = w_n^{\mathrm{tr}}$ is the transpose of w_n and so $\operatorname{tr} w_n = \operatorname{tr} \theta(w_n)$. However, we may reduce to the symmetric case as follows: Firstly, it suffices to prove the equality on the Zariski-dense open subset of (A, B) where A is diagonalizable. There, we may assume that

$$A = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}$$

is diagonal by conjugating the word. Next, if we write

$$B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

then simultaneously conjugating by a diagonal matrix

$$\Lambda = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix},$$

we preserve the trace, keep A unchanged and B changes to

$$\Lambda B \Lambda^{-1} = \begin{pmatrix} x & y\lambda^2 \\ z/\lambda^2 & w \end{pmatrix}.$$

Now choose λ so that $z/\lambda^2 = y\lambda^2$ to get both A and B symmetric. ∎

Remark: See Buser [6] for a geometric description of this involution.

3. Trace polynomials

Our goal in this section is to give a tractable expression for the trace of the word $w(\mathbf{r}, \mathbf{m}) = A^{r_1} B^{m_1} \cdots A^{r_n} B^{m_n}$. We denote by $R_2 = \mathrm{SL}(2, \mathbf{C}) \times \mathrm{SL}(2, \mathbf{C})$, the set of ordered pairs of matrices (A, B), on which $\mathrm{SL}(2, \mathbf{C})$ acts by simultaneous conjugation. Since the trace of a word $w(\mathbf{r}, \mathbf{m})$ depends only on the orbit of (A, B) under this action, we will find a convenient transversal to the orbits of $\mathrm{SL}(2, \mathbf{C})$ on which we will compute the trace $\operatorname{tr} w(\mathbf{r}, \mathbf{m})$.

PROPOSITION 3.1: *The subset S of R_2 consisting of pairs (A, B), with $A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ diagonal, and $B = Z \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} Z^{-1}$, $Z = \begin{pmatrix} 1 & x \\ 1 & x+1 \end{pmatrix}$, gives a local transversal to the orbits of $\mathrm{SL}(2, \mathbf{C})$ on a Zariski-dense open subset of R_2. In particular the locally defined functions a, b, x on R_2 are algebraically independent.*

We first prove that S intersects almost all orbits: We take the open dense subset of R_2 consisting of (A,B) which are both diagonalizable, and have no common invariant line (these give the irreducible two-dimensional representations of F_2). Then we can conjugate A to be diagonal:

$$A=\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}, \quad \text{and write } B=Z\begin{pmatrix} b & 0 \\ 0 & b^{-1}\end{pmatrix}Z^{-1}.$$

Changing Z by right multiplication by a diagonal matrix does not change B. We may further simultaneously conjugate A and B by a diagonal matrix D. This leaves

$$A=\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}$$

unchanged and replaces B by $DBD^{-1}=(DZ)B(DZ)^{-1}$, and so changing Z to DZD' with D, D' diagonal keeps us in the same orbit. To classify possible choices of Z, we use:

LEMMA 3.1: *For*

$$Z=\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4\end{pmatrix}\in \mathrm{SL}(2,\mathbf{C}),$$

set $x(Z)=z_2z_3$. *Then for any diagonal matrices* $D,D'\in\mathrm{SL}(2,\mathbf{C})$ *we have* $x(DZD')=x(Z)$ *and conversely, if* Z, Z' *are two matrices such that* $x(Z)=x(Z')\neq 0,-1$ *then* $Z'=DZD'$, *and every* Z *with* $x(Z)\neq 0,-1$ *lies in a unique double coset represented by* $\begin{pmatrix} 1 & x \\ 1 & x+1\end{pmatrix}$, $x=x(Z)$.

Proof: If $D=\begin{pmatrix} t & 0 \\ 0 & t^{-1}\end{pmatrix}$, $D'=\begin{pmatrix} s & 0 \\ 0 & s^{-1}\end{pmatrix}$ and $Z=\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4\end{pmatrix}$ then the computation

$$DZD'=\begin{pmatrix} stz_1 & \frac{t}{s}z_2 \\ \frac{s}{t}z_3 & \frac{z_4}{st}\end{pmatrix}$$

shows that if $Z'=DZD'=\begin{pmatrix} z_1' & z_2' \\ z_3' & z_4'\end{pmatrix}$, then $z_2'z_3'=z_2z_3$, and moreover that if $z_1,z_3\neq 0$ we can choose s, t so that $z_1'=1=z_3'$. ∎

Since generic orbits are 3-dimensional while $\dim R_2=6$, the functions a, b, x, defined locally on R_2, are algebraically independent. This concludes the proof of Proposition 3.1. ∎

Using the coordinate a,b,x on the orbits we give a preliminary expression for $\mathrm{tr}\, w(\mathbf{r},\mathbf{m})$:

PROPOSITION 3.2: *Let*

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad B = Z \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} Z^{-1}, \quad Z = \begin{pmatrix} 1 & x \\ 1 & x+1 \end{pmatrix}.$$

For a word $w_n(\mathbf{r}, \mathbf{m}) = A^{r_1} B^{m_1} \cdots A^{r_n} B^{m_n}$, *we have*

1. $\operatorname{tr} w_n(\mathbf{r}, \mathbf{m})$ *is a polynomial in* x *of degree* n*:*

$$\operatorname{tr} w_n(\mathbf{r}, \mathbf{m}) = c_0(\mathbf{r}, \mathbf{m}) + c_1(\mathbf{r}, \mathbf{m})x + \cdots + c_n(\mathbf{r}, \mathbf{m})x^n. \tag{3.1}$$

2. *The constant term is given by*

$$c_0(\mathbf{r}, \mathbf{m}) = a^R b^M + a^{-R} b^{-M},$$

where $R = \sum r_j$, $M = \sum m_j$.

3. *The leading term is given by*

$$c_n(\mathbf{r}, \mathbf{m}) = \prod_{j=1}^{n} (a^{r_j} - a^{-r_j})(b^{m_j} - b^{-m_j}).$$

Proof: Clearly the trace is a polynomial in x, so we can compute the zeroth coefficient $c_0(\mathbf{r}, \mathbf{m})$ by setting $x = 0$. But then

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

is lower triangular, and then

$$w(\mathbf{r}, \mathbf{m}) = \begin{pmatrix} a^{\sum r_j} b^{\sum m_j} & 0 \\ * & a^{-\sum r_j} b^{-\sum m_j} \end{pmatrix}$$

which shows that $c_0(\mathbf{r}, \mathbf{m}) = a^R b^M + a^{-R} b^{-M}$.

To see that $\operatorname{tr} w_n(\mathbf{r}, \mathbf{m})$ is a polynomial of degree n in x, we will show that the n-th derivative $d^n w / dx^n$ is a constant. We first write

$$w_n(\mathbf{r}, \mathbf{m}) = L_1(x) L_2(x) \cdots L_n(x),$$

where

$$\begin{aligned} L_j(x) &= A^{r_j} B^{m_j} \\ &= \begin{pmatrix} a^{r_j}(b^{m_j} - b^{-m_j})x + a^{r_j} b^{m_j} & -a^{r_j}(b^{m_j} - b^{-m_j})x \\ a^{-r_j}(b^{m_j} - b^{-m_j})(x+1) & -a^{-r_j}(b^{m_j} - b^{-m_j})x + a^{-r_j} b^{-m_j} \end{pmatrix}. \end{aligned} \tag{3.2}$$

Then

$$\frac{dL_j}{dx} = (b^{m_j} - b^{-m_j}) \begin{pmatrix} a^{r_j} & -a^{r_j} \\ a^{-r_j} & -a^{-r_j} \end{pmatrix} \tag{3.3}$$

and therefore $d^2L_j/dx^2 = 0$. Hence on using the Leibnitz rule, we find that

$$\frac{d^n w_n(\mathbf{r},\mathbf{m})}{dx^n} = n! L_1' \cdots L_n' = \prod_{j=1}^{n}(b^{m_j} - b^{-m_j}) \prod_{j=1}^{n} \begin{pmatrix} a^{r_j} & -a^{r_j} \\ a^{-r_j} & -a^{-r_j} \end{pmatrix}$$

and in particular $d^n w_n(\mathbf{r},\mathbf{m})/dx^n$ is constant. Now we use the identity

$$\begin{pmatrix} u & -u \\ u^{-1} & -u^{-1} \end{pmatrix}\begin{pmatrix} v & -v \\ v^{-1} & -v^{-1} \end{pmatrix} = (v - v^{-1})\begin{pmatrix} u & -u \\ u^{-1} & -u^{-1} \end{pmatrix}$$

to see that

$$L_1' \cdots L_n' = \prod_{j=1}^{n}(b^{m_j} - b^{-m_j}) \prod_{j=2}^{n}(a^{r_j} - a^{-r_j})\begin{pmatrix} a^{r_1} & -a^{r_1} \\ a^{-r_1} & -a^{-r_1} \end{pmatrix}$$

and so $c_n(\mathbf{r},\mathbf{m}) = \operatorname{tr} L_1' \cdots L_n' = \prod_{j=1}^{n}(a^{r_j} - a^{-r_j})(b^{m_j} - b^{-m_j})$. ∎

Remark: Instead of expanding in powers of x as in 1, one can expand in the basis $x^{n-k}(x+1)^k$, $0 \le k \le n$:

$$\operatorname{tr} w(\mathbf{r},\mathbf{m}) = \sum_{k=0}^{n} d_k(\mathbf{r},\mathbf{m}) x^{n-k}(x+1)^k.$$

It turns out that this expansion has some extra symmetry properties: Each of the 4^n monomials $\prod_{i=1}^{n} a^{\epsilon_i r_i} b^{\eta_i m_i}$, $\epsilon_i, \eta_j = \pm 1$, appears in exactly one of the coefficients d_k, and the coefficient with which it appears is $\prod_{j=1}^{n} \epsilon_j \eta_j$. Since we make no use of this fact we will omit the proof.

Definition 3.1: We say $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbf{Z}^n$ in **non-singular** if $r_k \neq \sum_{j\in S} r_j$ for all k and $S \subseteq \{1, \ldots, n\}$, $S \neq \{k\}$.

In particular, all the r_j are distinct, and $\sum_{j\in S} r_j \neq 0$ if S is non-empty.

COROLLARY 3.1: *If* $\mathbf{r}$, $\mathbf{m}$ *are non-singular then* $\operatorname{tr} w_n(\mathbf{r},\mathbf{m}) = \operatorname{tr} w_{n'}(\mathbf{r}',\mathbf{m}')$ *implies that* $n' = n$, *and either* $\mathbf{r}' = (r_1', \ldots, r_n')$ *is a permutation of* $\mathbf{r}$ *and* $\mathbf{m}'$ *a permutation of* $\mathbf{m}$, *or else* $\mathbf{r}'$ *is a permutation of* $-\mathbf{r}$ *and* $\mathbf{m}'$ *a permutation of* $-\mathbf{m}$.

Remark: It was already known [9] that without assuming $\mathbf{r}, \mathbf{m}$ are non-singular we need $n = n'$ and the absolute values of r_j' have to be a permutation of the $|r_j|$, and likewise for $\mathbf{m}'$. The above goes further in the case of $\mathbf{r}$, $\mathbf{m}$ non-singular since it excludes any sign changes other than replacing $(\mathbf{r},\mathbf{m})$ by $(-\mathbf{r},-\mathbf{m})$.

Proof: If $\operatorname{tr} w_n(\mathbf{r},\mathbf{m}) = \operatorname{tr} w_{n'}(\mathbf{r}',\mathbf{m}')$ then by comparing the degree in x we see that we need $n' = n$ and $c_n(\mathbf{r},\mathbf{m}) = c_n(\mathbf{r}',\mathbf{m}')$, i.e.

$$\prod_{j=1}^{n}(a^{r_j} - a^{-r_j})(b^{m_j} - b^{-m_j}) = \prod_{j=1}^{n}(a^{r'_j} - a^{-r'_j})(b^{m'_j} - b^{-m'_j}).$$

This forces $r'_j = \epsilon_j r_j$, $m'_j = \eta_j m_j$ with $\epsilon_i, \eta_j = \pm 1$ (this much is to be found in [9] and does not assume $\mathbf{r},\mathbf{m}$ non-singular). Now we further know that $c_0(\mathbf{r},\mathbf{m}) = c_0(\mathbf{r}',\mathbf{m}')$, i.e.

$$a^R b^M + a^{-R} b^{-M} = a^{R'} b^{M'} + a^{-R'} b^{-M'}.$$

This forces (R', M') to equal either (R, M) or $(-R, -M)$.

Suppose first that $R' = \sum \epsilon_j r_j = R = \sum r_j$, or equivalently

$$\sum_{j:\epsilon_j=-1} r_j = 0.$$

Since $\mathbf{r}$ is generic this forces the set of j such that $\epsilon_j = -1$ to be empty, i.e. $\mathbf{r}'$ is a permutation of $\mathbf{r}$. Also, in the case $R' = R$ we need $M' = M$ and the same argument shows that $\mathbf{m}'$ is a permutation of $\mathbf{m}$.

Next, suppose that $R' = -R$. Then arguing as above we find

$$\sum_{j:\epsilon_j=+1} r_j = 0$$

and since $\mathbf{r}$ is non-singular, all $\epsilon_j = -1$, which means that $\mathbf{r}'$ is a permutation of $-\mathbf{r}$, and as above $\mathbf{m}'$ is a permutation of $-\mathbf{m}$. ∎

4. The first variation of the trace

The main result of this section is a formula for the coefficient $c_1(\mathbf{r},\mathbf{m})$ of 1, which we can think of as the first variation of $\operatorname{tr} w(\mathbf{r},\mathbf{m})$ as we move in from the sub-variety of reducible representations ($x = 0$).

THEOREM 4.1: *The first variation of* $\operatorname{tr} w(\mathbf{r},\mathbf{m})$ *is given by*

$$c_1(\mathbf{r},\mathbf{m}) = c_1^{inv}(\mathbf{r},\mathbf{m}) - c'_1(\mathbf{r},\mathbf{m})$$

with $c_1^{inv}(\mathbf{r},\mathbf{m})$ *invariant under all permutations, and*

$$c'_1(\mathbf{r},\mathbf{m}) = \sum_{1\le i<j\le n} u_{i,j}(\mathbf{r},\mathbf{m}) + u_{i,j}(-\mathbf{r},-\mathbf{m})$$

where for $i < j$,

$$u_{i,j}(\mathbf{r},\mathbf{m}) = (1-b^{2m_i})(1-b^{2m_j})a^{R-2(r_{i+1}+\cdots+r_j)}b^{M-2(m_i+m_{i+1}+\cdots+m_j)}.$$

Proof of Theorem 4.1: We begin by writing $w_n(\mathbf{r},\mathbf{m}) = L_1(x)L_2(x)\cdots L_n(x)$, with $L_j(x)$ given by (3.2). Then

$$c_1(\mathbf{r},\mathbf{m}) = \operatorname{tr}\frac{dw_n}{dx}|_{x=0} = \sum_{j=1}^{n} L_1(0)\cdots L_{j-1}(0)L_j'(0)L_{j+1}(0)\cdots L_n(0)$$

with

$$L_j(0) = \begin{pmatrix} a^{r_j}b^{m_j} & \\ a^{-r_j}(b^{m_j}-b^{-m_j}) & a^{-r_j}b^{-m_j}\end{pmatrix}$$

and as in (3.3)

$$L_j'(0) = (b^{m_j}-b^{-m_j})\begin{pmatrix} a^{r_j} & -a^{r_j} \\ a^{-r_j} & -a^{-r_j}\end{pmatrix}.$$

LEMMA 4.1:

$$\begin{pmatrix} a_1 & \\ c_1 & a_1^{-1}\end{pmatrix}\begin{pmatrix} a_2 & \\ c_2 & a_2^{-1}\end{pmatrix}\cdots\begin{pmatrix} a_n & \\ c_n & a_n^{-1}\end{pmatrix} = \begin{pmatrix} a_1a_2\cdots a_n & \\ t_n & a_1^{-1}a_2^{-1}\cdots a_n^{-1}\end{pmatrix}$$

where $t_n = \sum_{k=1}^{n} a_1^{-1}\cdots a_{k-1}^{-1}c_k a_{k+1}\cdots a_n$.

Proof: By induction: Denoting the product by T_n, we have

$$T_n = T_{n-1}\begin{pmatrix} a_n & \\ c_n & a_n^{-1}\end{pmatrix}$$

and so

$$\begin{aligned} t_n &= a_n t_{n-1} + a_1^{-1}\cdots a_{n-1}^{-1}c_n \\ &= a_n\sum_{k=1}^{n-1} a_1^{-1}\cdots a_{k-1}^{-1}c_k a_{k+1}\cdots a_{n-1} + a_1^{-1}\cdots a_{n-1}^{-1}c_n \\ &= \sum_{k=1}^{n} a_1^{-1}\cdots a_{k-1}^{-1}c_k a_{k+1}\cdots a_n \end{aligned}$$

as required. ∎

In our case $a_j = a^{r_j}b^{m_j}$, $c_j = a^{-r_j}(b^{m_j}-b^{-m_j})$, and so for $j \geq 2$ we have

$$L_1(0)\cdots L_{j-1}(0) = \begin{pmatrix} a^{r_1+\cdots+r_{j-1}}b^{m_1+\cdots+m_{j-1}} & 0 \\ s_j & a^{-r_1+\cdots-r_{j-1}}b^{-m_1+\cdots-m_{j-1}}\end{pmatrix}$$

with

(4.1)

$$s_j = \sum_{k=1}^{j-1}(b^{m_k} - b^{-m_k})a^{-r_1\cdots-r_k+r_{k+1}+\cdots+r_{j-1}}b^{-m_1-\cdots-m_{k-1}+m_{k+1}+\cdots+m_{j-1}}$$
$$= \sum_{k=1}^{j-1}(1 - b^{-2m_k})a^{-r_1\cdots-r_k+r_{k+1}+\cdots+r_{j-1}}b^{-m_1-\cdots-m_{k-1}+(m_k+\cdots+m_{j-1})}$$

and likewise for $j \leq n-1$

$$L_{j+1}(0)\cdots L_n(0) = \begin{pmatrix} a^{r_{j+1}+\cdots+r_n}b^{m_{j+1}+\cdots+m_n} & 0 \\ t_j & a^{-r_{j+1}+\cdots-r_n}b^{-m_{j+1}+\cdots-m_n} \end{pmatrix}$$

with

(4.2)

$$t_j = \sum_{k=j+1}^{n}(b^{m_k} - b^{-m_k})a^{-r_{j+1}-\cdots-r_k+r_{k+1}+\cdots+r_n}b^{-m_{j+1}-\cdots-m_{k-1}+m_{k+1}+\cdots+m_n}$$
$$= \sum_{k=j+1}^{n}(b^{2m_k} - 1)a^{-r_{j+1}-\cdots-r_k+r_{k+1}+\cdots+r_n}b^{-m_{j+1}-\cdots-m_k+m_{k+1}+\cdots+m_n}.$$

Thus

$$\begin{aligned}
&L_1(0)\cdots L_{j-1}(0)L_j'(0)L_{j+1}(0)\cdots L_n(0)\\
=&\begin{pmatrix} a^{r_1+\cdots+r_{j-1}}b^{m_1+\cdots+m_{j-1}} & 0 \\ s_j & a^{-r_1+\cdots-r_{j-1}}b^{-m_1+\cdots-m_{j-1}} \end{pmatrix}\\
&\times (b^{m_j} - b^{-m_j})\left(\begin{pmatrix} a^{r_j} & 0 \\ a^{-r_j} & -a^{-r_j} \end{pmatrix} + \begin{pmatrix} 0 & -a^{r_j} \\ 0 & 0 \end{pmatrix}\right)\\
&\times \begin{pmatrix} a^{r_{j+1}+\cdots+r_n}b^{m_{j+1}+\cdots m_n} & 0 \\ t_j & a^{-r_{j+1}+\cdots-r_n}b^{-m_{j+1}-\cdots-m_n} \end{pmatrix}\\
=&(b^{m_j} - b^{-m_j})\begin{pmatrix} a^R b^{M-m_j} & 0 \\ * & -a^{-R}b^{-M+m_j} \end{pmatrix}\\
&-(b^{m_j} - b^{-m_j})\begin{pmatrix} 0 & a^{r_1+\cdots+r_j}b^{m_1+\cdots m_{j-1}} \\ 0 & a^{r_j}s_j \end{pmatrix}\\
&\quad\times \begin{pmatrix} a^{r_{j+1}+\cdots+r_n}b^{m_{j+1}+\cdots+m_n} & 0 \\ t_j & a^{-r_{j+1}+\cdots-r_n}b^{-m_{j+1}-\cdots-m_n} \end{pmatrix}\\
=&(b^{m_j} - b^{-m_j})\begin{pmatrix} a^R b^{M-m_j} & 0 \\ * & -a^{-R}b^{-M+m_j} \end{pmatrix}\\
&-(b^{m_j} - b^{-m_j})\begin{pmatrix} a^{r_1+\cdots+r_j}b^{m_1+\cdots+m_{j-1}}t_j & * \\ * & s_j a^{r_j-r_{j+1}-\cdots-r_n}b^{-m_{j+1}-\cdots-m_n} \end{pmatrix}.
\end{aligned}$$

Therefore

$$\begin{aligned}&\operatorname{tr} L_1(0)\cdots L_{j-1}(0)L_j'(0)L_{j+1}(0)\cdots L_n(0)\\ =&(b^{m_j}-b^{-m_j})(a^Rb^{M-m_j}-a^{-R}b^{-M+m_j})\\ &-(b^{m_j}-b^{-m_j})\left(a^{r_1+\dots+r_j}b^{m_1+\dots+m_{j-1}}t_j+s_ja^{r_j-r_{j+1}-\dots-r_n}b^{-m_{j+1}-\dots-m_n}\right).\end{aligned}$$

Inserting the expressions (4.1), (4.2) for s_j, t_j we find that

$$\begin{aligned}&\operatorname{tr} L_1(0)\cdots L_{j-1}(0)L_j'(0)L_{j+1}(0)\cdots L_n(0)\\ =&a^Rb^M(1-b^{-2m_j})+a^{-R}b^{-M}(1-b^{2m_j})\\ &-(b^{2m_j}-1)\sum_{k=j+1}^{n} a^{r_1+\dots+r_j-r_{j+1}-\dots-r_k+r_{k+1}+\dots+r_n}\\ &\qquad\qquad\times b^{m_1+\dots+m_{j-1}-m_j-\dots-m_k+m_{k+1}+\dots m_n}(b^{2m_k}-1)\\ &-(1-b^{-2m_j})\sum_{k=1}^{j-1}a^{-r_1-\dots-r_k+r_{k+1}+\dots r_j-r_{j+1}-\dots-r_n}\\ &\qquad\qquad\times b^{-m_1-\dots-m_{k-1}+m_k+\dots+m_j-m_{j+1}-\dots-m_n}(1-b^{-2m_k})\end{aligned}$$

(with obvious modifications for $j=1$ and $j=n$). Thus

$$c_1 = c_1^{inv} - c_1'$$

with

$$c_1^{inv} = a^Rb^M\sum_{j=1}^{n}(1-b^{-2m_j}) + a^{-R}b^{-M}\sum_{j=1}^{n}(1-b^{2m_j})$$

is invariant under all permutations, and

$$\begin{aligned}c_1' =&\sum_{j<k} a^{R-2(r_{j+1}+\dots+r_k)}b^{M-2(m_j+\dots+m_k)}(1-b^{2m_j})(1-b^{2m_k})\\ &+\sum_{j<k} a^{-R+2(r_{j+1}+\dots+r_k)}b^{-M+2(m_j+\dots+m_k)}(1-b^{-2m_j})(1-b^{-2m_k})\\ =&\sum_{j<k} u_{j,k}(\mathbf{r},\mathbf{m}) + u_{j,k}(-\mathbf{r},-\mathbf{m})\end{aligned}$$

as required. This proves Theorem 4.1. ∎

5. The main theorem

We now try to classify, for given $(\mathbf{r},\mathbf{m})$, all words $w(\mathbf{r}',\mathbf{m}')$ with $\operatorname{tr} w(\mathbf{r}',\mathbf{m}') = \operatorname{tr} w(\mathbf{r},\mathbf{m})$. From [9] (see remark after Corollary 3.1) we know that necessarily $n' = n$ and $|r_j'|$ are a permutation of the $|r_i|$, and likewise for $\mathbf{m}'$. Assume now that $\mathbf{r},\mathbf{m}$ are non-singular. Then by Corollary 3.1, either $\mathbf{r}' = (r_1',\dots,r_n')$ is a permutation of $\mathbf{r}$ and $\mathbf{m}'$ a permutation of $\mathbf{m}$, or else $\mathbf{r}'$ is a permutation of $-\mathbf{r}$ and $\mathbf{m}'$ a permutation of $-\mathbf{m}$; by replacing $w(\mathbf{r}',\mathbf{m}')$ by $w(-\mathbf{r}',-\mathbf{m}') = \theta(w(\mathbf{r}',\mathbf{m}'))^{-1}$ we may assume the former. In order to prove Theorem 1.1, it remains to determine which permutations $(\sigma,\sigma') \in S_n \times S_n$ preserve the trace of $w(\mathbf{r},\mathbf{m})$.

As examples we have conjugations in the group, which correspond to simultaneous cyclic permutations of the exponents: Thus if we set $\omega = (1,2,\dots,n)$ then $\hat{\omega}^k = (\omega^k,\omega^k) : 0 \le k < n$ preserve the trace. In addition, the involution θ induces a permutation of the indices (which we denote by the same letter) that also preserves traces. Let G_n denote the subgroup of $S_n \times S_n$ generated by $\hat{\omega}$ and θ. Our main result is:

THEOREM 5.1: *If $\mathbf{r}$, $\mathbf{m}$ are non-singular then the only permutations preserving the trace of $w_n(\mathbf{r},\mathbf{m})$ are the group $G_n = \{\hat{\omega}^k, \theta\hat{\omega}^k : k = 0,\dots,n-1\}$.*

Proof of Theorem 5.1: We show that if $\mathbf{r}$ and $\mathbf{m}$ are non-singular and if $\operatorname{tr} w(\sigma\mathbf{r},\sigma'\mathbf{m}) = \operatorname{tr} w(\mathbf{r},\mathbf{m})$ then $(\sigma,\sigma') \in G_n$. Now if (σ,σ') preserves the trace, then since a,b,x are algebraically independent, then also $c_1(\sigma\mathbf{r},\sigma'\mathbf{m}) = c_1(\mathbf{r},\mathbf{m})$ and since $c_1 = c_1^{inv} - c_1'$ with c_1^{inv} invariant under all permutations, we need that c_1' is also preserved. Now by Theorem 4.1, $c_1' = \sum_{i<j} u_{i,j}(\mathbf{r},\mathbf{m}) + u_{i,j}(-\mathbf{r},-\mathbf{m})$. We single out in this the sum of the terms $u_{i,i+1}(\mathbf{r},\mathbf{m})$ and also the term $u_{1,n}(-\mathbf{r},-\mathbf{m})$:

$$\begin{aligned} S(\mathbf{r},\mathbf{m}) &= u_{1,n}(-\mathbf{r},-\mathbf{m}) + \sum_{i=1}^{n-1} u_{i,i+1}(\mathbf{r},\mathbf{m}) \\ &= a^R b^M \sum_{i=1}^{n} (1-b^{-2m_{i-1}})(1-b^{-2m_i})a^{-2r_i} \end{aligned}$$

(with the convention $m_0 = m_n$).

We first claim that for $\mathbf{r}$ non-singular, if $c_1'(\mathbf{r},\mathbf{m}) = c_1'(\sigma\mathbf{r},\sigma'\mathbf{m})$ then $S(\sigma\mathbf{r},\sigma'\mathbf{m}) = S(\mathbf{r},\mathbf{m})$. To see this, we must show that the powers of a, appearing in $S(\sigma\mathbf{r},\sigma'\mathbf{m})$ cannot occur in $c_1'(\mathbf{r},\mathbf{m}) - S(\mathbf{r},\mathbf{m})$. This is done in the following Lemma:

LEMMA 5.1: *For* $\mathbf{r}$ *non-singular, if* $i < j$ *is such that* $(i,j) \neq (k,k+1)$ *and* $(i,j) \neq (1,n)$ *then for any permutation* $\sigma \in S_n$ *the exponents* $R - 2r_k$, $k = 1, \dots, n$ *are distinct from any of the exponents* $\pm(R - 2(r_{\sigma(i+1)} + r_{\sigma(i+2)} + \cdots + r_{\sigma(j)}))$ *with* $j \neq i+1$.

Proof: Suppose first that for some $1 \le k \le n-1$ and $1 \le i < j \le n$ we have

$$R - 2r_k = R - 2(r_{\sigma(i+1)} + \cdots + r_{\sigma(j)}).$$

Then $r_k = r_{\sigma(i+1)} + \cdots + r_{\sigma(j)}$ and since $\mathbf{r}$ is non-singular we need that $j = i+1$ (and also $k = \sigma(i)$). The other possibility to check is

$$R - 2r_k = -R + 2(r_{\sigma(i+1)} + \cdots + r_{\sigma(j)}),$$

that is

$$R - r_k = r_{\sigma(i+1)} + \cdots + r_{\sigma(j)}$$

or that

$$r_k = \sum_{t \neq \sigma(i+1), \dots, \sigma(j)} r_t.$$

The assumption that $\mathbf{r}$ is non-singular means precisely that this cannot happen unless $i = 1$, $j = n$ (and also $\sigma(1) = k$) as required. ∎

We can now conclude that for $\mathbf{r}$ non-singular, if $\operatorname{tr} w(\sigma\mathbf{r}, \sigma'\mathbf{m}) = \operatorname{tr} w(\mathbf{r}, \mathbf{m})$ then

$$S_n(\sigma\mathbf{r}, \sigma'\mathbf{m}) = S_n(\mathbf{r}, \mathbf{m}). \tag{5.1}$$

Now assume that $\mathbf{m}$ is such that m_j are distinct, and $(\sigma, \sigma') \in S_n \times S_n$ is such that $S_n(\sigma\mathbf{r}, \sigma'\mathbf{m}) = S_n(\mathbf{r}, \mathbf{m})$. We want to show that $(\sigma, \sigma') \in G_n$. By conjugating, we can assume that $w(\sigma\mathbf{r}, \sigma'\mathbf{m})$ ends in b^{m_n}, i.e. that $\sigma'(n) = n$. A further reduction is that, if necessary, applying θ we may assume that $\sigma(n) \neq 1$. We will now show that in fact $(\sigma, \sigma') = (\mathrm{id}, \mathrm{id})$. This will prove Theorem 5.1.

Now (5.1) means that (with the convention $m_0 = m_n$)

(5.2)
$$\sum_{i=1}^{n} (1 - b^{-2m_{i-1}})(1 - b^{-2m_i}) a^{-2r_i} = \sum_{i=1}^{n} (1 - b^{-2m_{\sigma'(i-1)}})(1 - b^{-2m_{\sigma'(i)}}) a^{-2r_{\sigma(i)}}.$$

Setting $y = b^{-2}$, $z = a^{-2}$, we will show:

LEMMA 5.2: *If* $\mathbf{r} = (r_1, \ldots, r_n)$ *are distinct and* $\mathbf{m} = (m_1, \ldots, m_n)$ *are distinct, and* $(\sigma, \sigma') \in S_n \times S_n$ *is such that* $\sigma'(n) = n$, $\sigma(n) \neq 1$, *and satisfies*

$$\sum_{i=1}^{n} (1 - y^{m_{i-1}})(1 - y^{m_i}) z^{r_i} = \sum_{i=1}^{n} (1 - y^{m_{\sigma'(i-1)}})(1 - y^{m_{\sigma'(i)}}) z^{r_{\sigma(i)}}, \tag{5.3}$$

then $(\sigma, \sigma') = (\mathrm{id}, \mathrm{id})$.

Proof: We focus on the two summands containing $(1 - y^{m_n}) = (1 - y^{m_{\sigma'(n)}})$. Since y, z are algebraically independent, the sum of the two terms on each side of (5.3) has to coincide, i.e.

$$\begin{aligned} &(1 - y^{m_{n-1}})(1 - y^{m_n}) z^{r_n} + (1 - y^{m_n})(1 - y^{m_1}) z^{r_1} \\ =&(1 - y^{m_{\sigma'(n-1)}})(1 - y^{m_n}) z^{r_{\sigma(n)}} + (1 - y^{m_n})(1 - y^{m_{\sigma'(1)}}) z^{r_{\sigma(1)}}. \end{aligned} \tag{5.4}$$

Since r_j are distinct and $\sigma(n) \neq 1$, we must have $\sigma(1) = 1$ and, comparing powers of y, we also see that $\sigma'(n-1) = n-1$, $\sigma'(1) = 1$.

Next, we omit the two terms (5.4) in (5.3) to get an equality of sums of $n-2$ terms:

$$\sum_{j=2}^{n-1} (1 - y^{m_{j-1}})(1 - y^{m_j}) z^{r_j} = \sum_{j=2}^{n-1} (1 - y^{m_{\sigma'(j-1)}})(1 - y^{m_{\sigma'(j)}}) z^{r_{\sigma(j)}} \tag{5.5}$$

and $\sigma'(n-1) = n-1$, $\sigma(1) = 1 = \sigma(1)'$. We will prove by induction on i that $\sigma'(i) = i = \sigma(i)$. For $i = 1$, we already have $\sigma(1) = 1 = \sigma'(1)$ and, comparing the summands containing $y^{m_1} = y^{m_{\sigma'(1)}}$, we find

$$(1 - y^{m_1})(1 - y^{m_2}) z^{r_2} = (1 - y^{m_1})(1 - y^{m_{\sigma'(2)}}) z^{r_{\sigma(2)}}$$

and therefore $\sigma(2) = 2 = \sigma'(2)$.

Continuing in this way, suppose that we showed that $\sigma(j) = j = \sigma'(j)$ for all $j < i$. We will now show that $\sigma(i) = i = \sigma'(i)$. We can omit the identical summands for $j = 1, \ldots i-1$ in both sides of (5.5) to find

$$\sum_{j=i}^{n-1} (1 - y^{m_{j-1}})(1 - y^{m_j}) z^{r_j} = \sum_{j=i}^{n-1} (1 - y^{m_{\sigma'(j-1)}})(1 - y^{m_{\sigma'(j)}}) z^{r_{\sigma(j)}}.$$

The only summand involving $m_{i-1} = m_{\sigma'(i-1)}$ is the one for $j = i$, which gives

$$(1 - y^{m_{i-1}})(1 - y^{m_i}) z^{r_i} = (1 - y^{m_{i-1}})(1 - y^{m_{\sigma'(i)}}) z^{r_{\sigma(i)}},$$

and equating powers of y and z we get $\sigma(i) = i = \sigma'(i)$ as required. This shows that $\sigma = \mathrm{id} = \sigma'$. ∎

References

[1] R. Abraham, *Bumpy metrics*, Proceedings of Symposia in Pure Mathematics **14**, American Mathematical Society, Providence, R.I., 1970, pp. 1–3.

[2] R. Aurich and F. Steiner, *Energy-level statistics of the Hadamard–Gutzwiller ensemble*, Physica D **43** (1990), 155–180.

[3] M. V. Berry, *Semiclassical theory of spectral rigidity*, Proceedings of the Royal Society of London, Series A **400** (1985), 229–251.

[4] E. Bogomolny, B. Georgeot, M.-J. Giannoni and C. Schmit, *Chaotic billiards generated by arithmetic groups*, Physical Review Letters **69** (1992), 1477–1480.

[5] E. Bogomolny, F. Leyvraz and C. Schmit, *Distribution of eigenvalues for the modular group*, to appear in Communications in Mathematical Physics.

[6] P. Buser, *Geometry and Spectra of Compact Riemann Surfaces*, Birkhäuser, Boston, 1992.

[7] M. Dehn, *Transformation der Kurven auf zweiseitigen Flächen*, Mathematische Annalen **72** (1912), 413–421.

[8] D. A. Hejhal, *The Selberg Trace Formula for* PSL$(2,\mathbf{R})$, Lecture Notes in Mathematics **548**, Springer-Verlag, Berlin, Heidelberg, New York, 1976.

[9] R. Horowitz, *Characters of free groups represented in the two-dimensional special linear group*, Communications on Pure and Applied Mathematics **25** (1972), 635–649.

[10] W. Luo and P. Sarnak, *Number variance for arithmetic hyperbolic surfaces*, Communications in Mathematical Physics **161** (1994), 419–432.

[11] B. Randol, *The length spectrum of a Riemann surface is always of unbounded multiplicity*, Proceedings of the American Mathematical Society **78** (1980), 455–456.

[12] P. Schmutz, *Arithmetic groups and the length spectrum of Riemann surfaces*, Duke Mathematical Journal **84** (1996), 199–215.

[13] H. Zieschang, E. Vogt and H.-D. Coldewey, *Surfaces and Planar Discontinuous Groups*, Lecture Notes in Mathematics **835**, Springer-Verlag, Berlin, 1980.