A GEOMETRIC CHARACTERIZATION OF ARITHMETIC FUCHSIAN GROUPS *

Slavyana Geninska, Enrico Leuzinger

November 26, 2009

Abstract

The trace set of a Fuchsian group Γ encodes the set of lengths of closed geodesics in the surface $\Gamma\backslash\mathbb{H}$. Luo and Sarnak showed that the trace set of a cofinite arithmetic Fuchsian group satisfies the bounded clustering property. Sarnak then conjectured that the B-C property actually characterizes arithmetic Fuchsian groups. Schmutz stated the even stronger conjecture that a cofinite Fuchsian group is arithmetic if its trace set has linear growth. He proposed a proof of this conjecture in the case when the group Γ contains at least one parabolic element, but unfortunately this proof contains a gap. In the present paper we point out this gap and we prove Sarnak's conjecture under the assumption that the Fuchsian group Γ contains parabolic elements.

1 Introduction

Let Γ be a Fuchsian group, i.e. a discrete subgroup of $PSL(2,\mathbb{R})$. Such a Γ acts properly discontinuously and isometrically on the hyperbolic plane $\mathbb{H}$ and $M = \Gamma\backslash\mathbb{H}$ is a Riemann surface. The *trace set of* Γ and the *trace set of* M are defined as follows:

$$\begin{aligned} \mathrm{Tr}(\Gamma) &:= \{\mathrm{tr}(T) \mid T \in \Gamma\}, \\ \mathrm{Tr}(M) &= \{\mathrm{tr}(a) := 2\cosh\frac{L(a)}{2} \mid a \text{ is a closed geodesic in } M \text{ of length } L(a)\}. \end{aligned}$$

These two subsets of $\mathbb{R}$ in fact coincide for torsion free Γ.

It is a general question whether certain classes of Fuchsian groups can be characterized by means of their trace sets or, equivalently, by the trace sets of the surfaces that they define. In this paper we are interested in characterizations of arithmetic Fuchsian groups. There is a classical characterization of (cofinite) arithmetic Fuchsian groups due to Takeuchi which is based on number theoretical properties of their trace sets [7].

Theorem 1.1 ([7])**.** *Let Γ be a cofinite Fuchsian group. Then Γ is derived from a quaternion algebra over a totally real algebraic number field if and only if Γ satisfies the following two conditions:*

(i) $K := \mathbb{Q}(\mathrm{Tr}(\Gamma))$ is an algebraic number field of finite degree and $\mathrm{Tr}(\Gamma)$ is contained in the ring of integers $\mathcal{O}_K$ of K.

*The final version of this article has been published in the *Duke Mathematical Journal*, Vol. 142, No. 1, published by Duke University Press.

(ii) For any embedding φ of K into $\mathbb{C}$, which is not the identity, $\varphi(\mathrm{Tr}(\Gamma))$ is bounded in $\mathbb{C}$.

Remark. If Γ is derived from a quaternion algebra over a totally real algebraic number field F, then F is equal to K as in the above theorem.

Theorem 1.2 ([7]). *Let Γ be a cofinite Fuchsian group and $\Gamma^{(2)}$ be the subgroup of Γ generated by the set $\{T^2 \mid T \in \Gamma\}$. Then Γ is an arithmetic Fuchsian group if and only if $\Gamma^{(2)}$ is derived from a quaternion algebra.*

W. Luo and P. Sarnak pointed out large scale properties of the behavior of the trace set of arithmetic Fuchsian groups. We say that the trace set of a Fuchsian group Γ satisfies the *bounded clustering* or *B-C property* iff there exists a constant $B(\Gamma)$ such that for all integers n the set $\mathrm{Tr}(\Gamma) \cap [n, n+1]$ has less than $B(\Gamma)$ elements. Further set

$$Gap(\Gamma) := \inf\{|a-b| \mid a, b \in \mathrm{Tr}(\Gamma), a \neq b\}.$$

In [3] Luo and Sarnak made a first step toward a new geometric characterization of arithmetic Fuchsian groups by proving the following result:

Theorem 1.3 ([3]). *Let Γ be a cofinite Fuchsian group.*

(i) If Γ is arithmetic, then $\mathrm{Tr}(\Gamma)$ satisfies the B-C property.

(ii) If Γ is derived from a quaternion algebra, then $Gap(\Gamma) > 0$.

Sarnak conjectured that the converse assertions of Theorem 1.3 also hold:

Conjecture 1.4 (Sarnak [5]). *Let Γ be a cofinite Fuchsian group.*

(i) If $\mathrm{Tr}(\Gamma)$ satisfies the B-C property, then Γ is arithmetic.

(ii) If $Gap(\Gamma) > 0$, then Γ is derived from a quaternion algebra.

In [6] P. Schmutz makes an even stronger conjecture using the linear growth of a trace set instead of the B-C property. The trace set of a Fuchsian group Γ is said to have *linear growth* iff there exist positive real constants C and D such that for every $n \in \mathbb{N}$

$$\#\{a \in \mathrm{Tr}(\Gamma) \mid a \leq n\} \leq D + nC.$$

Remark. If a Fuchsian group $\mathrm{Tr}(\Gamma)$ satisfies the B-C property, then $\mathrm{Tr}(\Gamma)$ has linear growth with $D = 0$ and $C = B(\Gamma)$. But the opposite is not true in general: linear $\not\Rightarrow$ B-C.

Conjecture 1.5 (Schmutz [6]). *Let Γ be a cofinite Fuchsian group. Then $\mathrm{Tr}(\Gamma)$ has linear growth iff Γ is arithmetic.*

In [6] Schmutz proposed a proof of Conjecture 1.5 in the case when Γ contains at least one parabolic element. But unfortunately the proof contains a gap as we will point out in Section 3.

The main result of this paper is Theorem 3.4 which confirms part (i) of Sarnak's Conjecture 1.4 under the assumption that the Fuchsian group Γ contains at least one parabolic element. We use techniques similar to those developed by Schmutz.

It remains an open question whether the gap in [6] can be closed. Observe that a positive answer would imply that there do *not* exist *cofinite* Fuchsian groups (with parabolic elements)

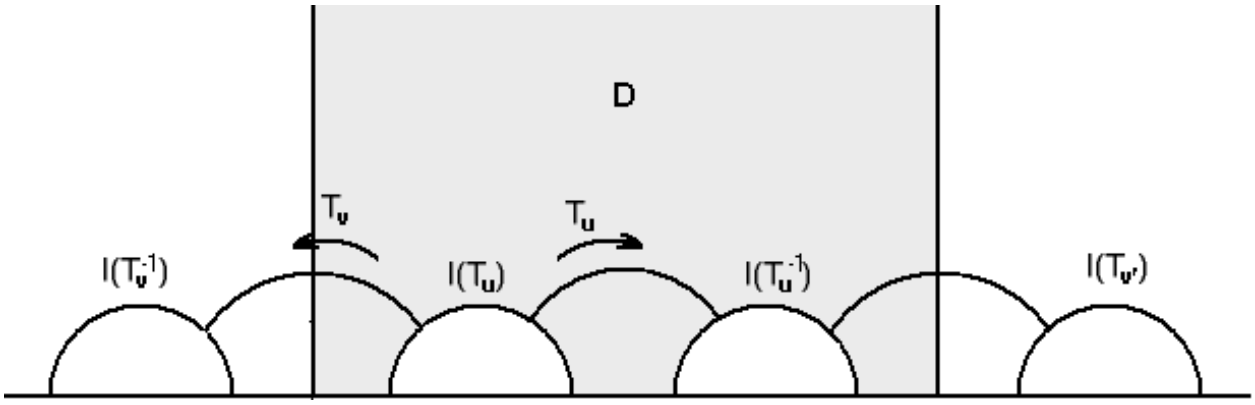

Figure 2.1: The case $\frac{a_1+d}{c} > 0$.

whose trace set grows linearly but does not satisfy the stronger B-C property. Furthermore we remark the conjectures of Sarnak and Schmutz remain completely open for cocompact Fuchsian groups.

A general reference for the notations and concepts in this paper are the books [2] and [4].

The authors would like to thank A. Deitmar for pointing out some inaccuracies in a previous version of this work and the referee for his constructive criticism.

2 Y-pieces and lengths of geodesics on them

In this section we prove (or list) some auxiliary results that are used later.

An *Y-piece* is a surface of constant curvature -1 and of signature $(0, 3)$, i.e. homeomorphic to a topological sphere with three points removed. For non-negative real numbers a, b, c we denote with $Y(a, b, c)$ an Y-piece with boundary geodesics of lengths a, b, c. It is well known that for given positive numbers a, b, c there exists an Y-piece $Y(a, b, c)$ which is unique up to isometry, see [1], Theorem 3.1.7.

We will say that an Y-piece $Y(a, b, c)$ is contained in a surface M iff $Y(a, b, c)$ is contained in a finite cover of M. Following [6], for a real number $a \geq 0$ we set $\mathrm{tr}(a) := 2\cosh\frac{a}{2}$. This is motivated by the following fact: if $T_a \in PSL(2, \mathbb{R})$ is a hyperbolic isometry giving rise to a closed geodesic of length a, then $\mathrm{tr}(T_a) = \mathrm{tr}(a)$.

In the next Proposition 2.1 we give sufficient conditions for two hyperbolic isometries to generate a group Γ such that $\Gamma\backslash\mathbb{H}$ contains an Y-piece $Y(u, v, 0)$.

Proposition 2.1. *Let u and v be non-negative real numbers. Further let T_u and T_v be elements of $PSL(2, \mathbb{R})$ such that $T_u = \begin{bmatrix} a_1 & b_1 \\ c & d \end{bmatrix}$ and $T_v = \begin{bmatrix} a_2 & b_2 \\ c & d \end{bmatrix}$, with $c \neq 0$ and such that for $\varepsilon = \pm 1$, $a_1 + d = \varepsilon\mathrm{tr}(u)$ and $a_2 + d = -\varepsilon\mathrm{tr}(v)$. Then $\Gamma = \langle T_u, T_v\rangle$ is a Fuchsian group and the surface $\Gamma\backslash\mathbb{H}$ contains an Y-piece $Y(u, v, 0)$.*

Proof. The group Γ contains a parabolic element $\begin{bmatrix} 1 & \varepsilon(\mathrm{tr}(u) + \mathrm{tr}(v))/c \\ 0 & 1 \end{bmatrix}$.

Indeed,

$$T := T_u T_v^{-1} = \begin{bmatrix} a_1 & b_1 \\ c & d \end{bmatrix} \begin{bmatrix} d & -b_2 \\ -c & a_2 \end{bmatrix} = \begin{bmatrix} 1 & b_1 a_2 - a_1 b_2 \\ 0 & 1 \end{bmatrix}$$

and

$$(b_1a_2 - a_1b_2)c = (a_1d - 1)a_2 - a_1(a_2d - 1) = (a_1 + d) - (a_2 + d) = \varepsilon(\mathrm{tr}(u) + \mathrm{tr}(v)).$$

The region D in Figure 2.1 is a fundamental domain for the Fuchsian group $\Gamma = \langle T, T_u\rangle = \langle T_u, T_v\rangle$ and $\Gamma\backslash D$ contains $Y(u, v, 0)$. □

Remark. The proposition remains true if T_u is an elliptic transformation of finite order, i.e. $a_1 + d \in (-2, 2)$. Then the Fuchsian group $\langle T_u, T_v\rangle$ contains a degenerated Y-piece $Y(u, v, 0)$, where u is an elliptic fixed point.

In the next corollary we use the notation of Proposition 2.1.

Corollary 2.2. *Let Γ be a Fuchsian group containing the parabolic element $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then for every element $T_u = \begin{bmatrix} a_1 & b_1 \\ c & d \end{bmatrix}$, $c \neq 0$, there exists $T_v \in \Gamma$, $v \geq 0$, such that $\langle T_u, T_v\rangle \backslash \mathbb{H}$ contains $Y(u, v, 0)$ with $\mathrm{tr}(u) = |a_1 + d|$.*

Proof. For any $k \in \mathbb{Z}$ we consider

$$T^kT_u = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c & d \end{bmatrix} = \begin{bmatrix} a_1 + kc & b_1 + kd \\ c & d \end{bmatrix}.$$

Pick $k' \in \mathbb{Z}$ such that $(a_1 + d)(a_1 + k'c + d) \leq 0$ and $|a_1 + k'c + d| \geq 2$. Then set $T_v := T^{k'}T_u$ and the claim follows from Proposition 2.1 and the previous remark. □

Corollary 2.3. *Let Γ be a Fuchsian group containing at least one parabolic element. Then for every non-parabolic element T_u in Γ there exists $T_v \in \Gamma$ such that $\langle T_u, T_v\rangle \backslash \mathbb{H}$ contains an Y-piece $Y(u, v, 0)$ with $\mathrm{tr}(u) = \mathrm{tr}(T_u)$.*

Proof. If Γ contains a parabolic element T_1 then, for some $R \in PSL(2, \mathbb{R})$, $RT_1R^{-1} = T$ or $RT_1^{-1}R^{-1} = T$ where $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. If $R\Gamma R^{-1}$ contains also an element $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ then A is a parabolic element because otherwise the group $\langle T, A\rangle$ would not be discrete. From Corollary 2.2 it follows that for every non-parabolic element RT_uR^{-1} in $R\Gamma R^{-1}$ there exists $RT_vR^{-1} \in R\Gamma R^{-1}$ such that $\langle RT_uR^{-1}, RT_vR^{-1}\rangle \backslash \mathbb{H}$ contains an Y-piece $Y(u, v, 0)$ with $\mathrm{tr}(u) = \mathrm{tr}(T_u)$. And hence for every non-parabolic element T_u in Γ there exists $T_v \in \Gamma$ such that $\langle T_u, T_v\rangle \backslash \mathbb{H}$ contains an Y-piece $Y(u, v, 0)$ with $\mathrm{tr}(u) = \mathrm{tr}(T_u)$. □

We next list several technical lemmas due to Schmutz which we need in the proof of Sarnak's conjecture.

Lemma 2.4 ([6])**.** *For all positive integers n, $Y(x, y, 0)$ contains $Y(\nu_n, y, 0)$, where*

$$\mathrm{tr}(\nu_n) = n(\mathrm{tr}(x) + \mathrm{tr}(y)) - \mathrm{tr}(y).$$

In particular, $\mathrm{Tr}(Y(x, y, 0))$ *contains the set* $\{\mathrm{tr}(\nu_n) : \ n = 1, 2, 3 \ldots\}$.

Remark. Lemma 2.4 is true even if $Y(x, y, 0)$ is a degenerated Y-piece where x corresponds to an elliptic fixed point and y is a closed geodesic. In that case $\mathrm{tr}(x)$ is equal to the trace of the generating elliptic element.

Lemma 2.5 ([6]). $\mathrm{Tr}(Y(x,0,0))$ *contains* $\mathrm{Tr}(Y(\lambda_k,\mu_m,0))$ *with* $\mathrm{tr}(\lambda_k) = k(\mathrm{tr}(x)+2)+2$ *and* $\mathrm{tr}(\mu_m) = m(\mathrm{tr}(x)+2)-2$ *for all pairs* (k,m), $k,m \in \mathbb{Z}^+$.

Lemma 2.6 ([6]). $\mathrm{Tr}(Y(x,y,0))$ *contains* $\mathrm{Tr}(Y(\nu,2y,0))$ *with* $\mathrm{tr}(\nu) = 2+\mathrm{tr}(x)\mathrm{tr}(y)$.

Lemma 2.7 ([6]). $\mathrm{Tr}(Y(x,y,0))$ *contains* $\mathrm{Tr}(Y(\nu,0,0))$ *where* $\mathrm{tr}(\nu) = (\mathrm{tr}(x)+\mathrm{tr}(y))^2-2$.

3 The growth of the length spectrum

In [6] Schmutz proposes a proof of Conjecture 1.5 under the assumption that the group Γ contains parabolic elements. Unfortunately the proof contains a gap as we will explain in this section. However, using ideas and methods similar to those in [6] we are able to prove (part of) Sarnak's Conjecture 1.4: Let Γ be a cofinite Fuchsian group, which contains parabolic elements. If Γ satisfies the B-C property, then Γ is arithmetic.

3.1 The attempt of Schmutz to prove Conjecture 1.5

For the results about arithmetic Fuchsian groups that are used in this section we refer to [2], Chapter 5.

Let Γ be a cofinite Fuchsian group with at least one parabolic element, i.e. $\Gamma\backslash\mathbb{H}$ is not compact. If Γ is derived from a quaternion algebra A, then A is not a division quaternion algebra and consequently A is a quaternion algebra over $\mathbb{Q}$. Hence, by Theorem 1.1 and the remark following it, in order to prove the second part of Conjecture 1.4 (in the case when Γ contains at least one parabolic element), it is enough to show that $Gap(\Gamma) > 0$ implies $\mathrm{Tr}(\Gamma) \subseteq \mathbb{Z}$. If one wishes to show that Γ is an arithmetic Fuchsian group it is enough to show that $\Gamma^{(2)}$ is derived from a quaternion algebra (Theorem 1.2). And since $\Gamma^{(2)}$ also contains at least one parabolic element it is sufficient to show that $\mathrm{Tr}(\Gamma^{(2)}) \subseteq \mathbb{Z}$ which is the same as to show that $\{\mathrm{tr}(a)^2 \mid a \in \Gamma\} \subseteq \mathbb{Z}$ because $\mathrm{tr}(a^2) = \mathrm{tr}(a)^2 - 2$.

The idea of a possible proof of Conjecture 1.5 is now the following: For an Y-piece $Y(a,b,c)$ we set $Gap(Y(a,b,c)) := Gap(\langle T_a, T_b\rangle)$, where T_a and T_b are isometries generating $Y(a,b,c)$ like in Proposition 2.1. From Corollary 2.3 we know that for every non-parabolic element T_x in Γ there exists $T_y \in \Gamma$ such that $\langle T_x, T_y\rangle\backslash\mathbb{H}$ contains an Y-piece $Y(x,y,0)$ with $\mathrm{tr}(x) = \mathrm{tr}(T_x)$. Since the trace of every parabolic transformation is equal to 2, it is enough to show that if $\mathrm{Tr}(\Gamma)$ has linear growth then, for every $Y(x,y,0)$, $\mathrm{tr}(x)^2$ and $\mathrm{tr}(y)^2$ are integers.

In [6] Schmutz proves the following two propositions:

Proposition 3.1 ([6]). $Gap(Y(x,0,0)) > 0$ *if and only if* $\mathrm{tr}(x)$ *is an integer.*

Proposition 3.2 ([6]). *If* $Gap(Y(x,y,0)) > 0$, *then the numbers* $\mathrm{tr}(x)^2$, $\mathrm{tr}(y)^2$ *and* $\mathrm{tr}(x)\mathrm{tr}(y)$ *are integers.*

Note that in the proof of Proposition 3.2 the condition $Gap(Y(x,y,0)) > 0$ is used only in case we need $Gap(Y(z,0,0)) > 0$ in order to apply Proposition 3.1 for an Y-piece $Y(z,0,0)$ contained in $Y(x,y,0)$. If $\mathrm{Tr}(\Gamma)$ has linear growth then $\mathrm{Tr}(Y(x,y,0))$ has linear growth for every Y-piece $Y(x,y,0)$ contained in $\Gamma\backslash\mathbb{H}$. Our aim is to prove that if $\mathrm{Tr}(Y(x,y,0))$ has linear growth then $\mathrm{tr}(x)^2$ and $\mathrm{tr}(y)^2$ are integers. The idea of Schmutz is to proceed as in the proof of Proposition 3.2, but instead of Proposition 3.1 to use the following

Claim 3.3. $\mathrm{Tr}(Y(x,0,0))$ *has linear growth if and only if* $\mathrm{tr}(x)$ *is an integer.*

Proposition 3.1 shows that $Gap(Y(x,0,0)) > 0$ if $\mathrm{tr}(x)$ is an integer and hence $\mathrm{Tr}(Y(x,0,0))$ has linear growth. So in order to prove Claim 3.3 it remains to show that if $\mathrm{Tr}(Y(x,0,0))$ has linear growth then $\mathrm{tr}(x) \in \mathbb{N}$, which is the same as to show that if $\mathrm{tr}(x)$ is not an integer then $\mathrm{Tr}(Y(x,0,0))$ has not linear growth.

If the real number $\mathrm{tr}(x)$ is not an integer it can be either rational or irrational. In [6] the author proposes the following proof in the case when $\mathrm{tr}(x)$ is rational: Assume that $z := \mathrm{tr}(x) + 2$ is not rational. By Lemma 2.5, $\mathrm{Tr}(Y(x,0,0))$ contains $\mathrm{Tr}(Y(\lambda_k, \mu_m, 0))$ with $\mathrm{tr}(\lambda_k) = k(\mathrm{tr}(x)+2)+2$ and $\mathrm{tr}(\mu_m) = m(\mathrm{tr}(x)+2)-2$ for all pairs (k,m), $k, m \in \mathbb{Z}^+$. Hence it follows from Lemma 2.6 that $\mathrm{Tr}(Y(x,0,0))$ contains $\mathrm{tr}(\mu_m)\mathrm{tr}(\lambda_k)+2$ and thus also the set

$$\{mkz^2 - 2(k-m)z - 2 \mid m, k \in \mathbb{Z}^+\}.$$

Since $z \notin \mathbb{Q}$, the numbers $mkz^2 - 2(k-m)z - 2$ are different for different pairs of positive integers. In this case we have that $\#\{a \in \mathrm{Tr}(Y(x,0,0)) \mid a \leq Nz^2\} \geq \frac{1}{2}\sum_{i=1}^{N} \sigma_0(i)$, where $\sigma_0(i)$ is the number of different positive divisors of i. It can be shown that

$$N \log N + N \geq \sum_{i=1}^{N} \sigma_0(i) = \sum_{j=1}^{N} \left[\frac{N}{j}\right] \geq N \log N - N$$

which means that $\sum_{i=1}^{N} \sigma_0(i)$ grows like $N \log N$ and in particular *not linear* (and in particular does *not* satisfy the B-C property). This proves Claim 3.3 in the case when z is not a rational number.

3.2 The gap in the proof of Claim 3.3 in [6]

Unfortunately the above argument breaks down in the case when $z = tr(x)+2$ is a *rational number* $\frac{a}{b}$ with $b > 1$ and $(a,b) = 1$, because $v_1 := m_1k_1z^2 - 2(k_1-m_1)z - 2$ and $v_2 := m_2k_2z^2 - 2(k_2-m_2)z - 2$ can be equal for different pairs (k_1, m_1) and (k_2, m_2). Indeed, assume that $v_1 = v_2$ or equivalently, since $z > 0$, that

$$(m_1k_1 - m_2k_2)z - 2(k_1 - m_1 - (k_2 - m_2)) = 0.$$

Now, if $Az + B = 0$ for some integers A and B and $z = \frac{a}{b}$, then A must not be 0, it can also be divisible by b. But if $|A| < b$ then $A = 0$ and thus $B = 0$ and as in the case when z is irrational we have $k_1 = k_2$ and $m_1 = m_2$. Therefore, since k_1, m_1, k_2 and m_2 are positive, we can guarantee that v_1 and v_2 are different for different pairs (k_1, m_1) and (k_2, m_2), if $m_1k_1 < b$ and $m_2k_2 < b$ and thus as in the case $z \notin \mathbb{Q}$ we get

$$\#\{y \in \mathrm{Tr}(Y(x,0,0)) \mid y \leq bz^2\} \geq \frac{1}{2}\sum_{i=1}^{b} \sigma_0(i) \geq \frac{1}{2}(b \log b - b).$$

From Lemma 2.7 it follows that $\mathrm{Tr}(Y(x,0,0))$ contains $\mathrm{Tr}(Y(x_2,0,0))$ with $\mathrm{tr}(x_2) = (\mathrm{tr}(x)+2)^2 - 2 = z^2 - 2$. By induction $\mathrm{Tr}(Y(x,0,0))$ contains $\mathrm{Tr}(Y(x_n,0,0))$ with $\mathrm{tr}(x_n) = z^{(2^n)} - 2$.

In [6] the author suggests to use the above estimates of the trace set for every $Y(x_n,0,0)$ (in this case $\mathrm{tr}(x_n)+2 = z^{2^n} = \frac{a^{2^n}}{b^{2^n}}$):

$$\#\{y \in \mathrm{Tr}(Y(x_n,0,0)) \mid y \leq b^{2^n} z^{2^{n+1}}\} \geq \frac{1}{2}\sum_{i=1}^{b^{2^n}} \sigma_0(i) \geq \frac{1}{2}(b^{2^n} \log b^{2^n} - b^{2^n}).$$

He claims that $\mathrm{Tr}(Y(x,0,0))$ has not linear growth because for every $n \in \mathbb{N}$

$$\begin{aligned}\#\{y \in \mathrm{Tr}(Y(x,0,0)) \mid y \leq b^{2^n} z^{2^{n+1}}\} &\geq \#\{y \in \mathrm{Tr}(Y(x_n,0,0)) \mid y \leq b^{2^n} z^{2^{n+1}}\} \\ &\geq \frac{1}{2}\sum_{i=1}^{b^{2^n}} \sigma_0(i) \geq \frac{1}{2}(b^{2^n}\log b^{2^n} - b^{2^n}).\end{aligned}$$

If $z^{2^{n+1}}$ were a constant then this argumentation would work. However, $z^{2^{n+1}}$ also grows when n grows! An immediate counter-example are the Y-pieces $Y(x = z-2,0,0)$ with $z^2 = \frac{a^2}{b^2} > b$: If the estimate

$$\#\{y \in \mathrm{Tr}(Y(x,0,0)) \mid y \leq b^{2^n} z^{2^{n+1}}\} \geq \frac{1}{2}\sum_{i=1}^{b^{2^n}} \sigma_0(i)$$

implies non-linear growth then there exists $n_0 \in \mathbb{N}$ such that for infinitely many $n \geq n_0$ the inequality $b^{2^n} z^{2^{n+1}} \leq \frac{1}{2}\sum_{i=1}^{b^{2^n}} \sigma_0(i)$ holds. But this is not the case when $z^2 > b$. In fact, for all positive integers n, one has in that case

$$b^{2^n} z^{2^{n+1}} = b^{2^n}(z^2)^{2^n} > b^{2^n} b^{2^n} > \frac{1}{2} b^{2^n}(\log b^{2^n} + 1) \geq \frac{1}{2}\sum_{i=1}^{b^{2^n}} \sigma_0(i).$$

At first view a possible reason why the above considerations did not suffice to prove the non-linear growth of $\mathrm{Tr}(Y(x,0,0))$ might be that not enough elements of the set

$$S_n = \{mkz^{2^{n+1}} - 2(k-m)z^{2^n} - 2 \mid m,k \in \mathbb{Z}^+\}$$

have been taken into account. But it turns out that even in the union $\bigcup_{n=0}^{\infty} S_n$ there are not enough different numbers to guarantee non-linear growth of $\mathrm{Tr}(Y(x,0,0))$. Indeed, every $y \in S_0$ has the form

$$mk\frac{a^2}{b^2} - 2(k-m)\frac{a}{b} - 2 = \frac{a}{b^2}(mka - 2(k-m)b) - 2.$$

Hence

$$S_0 \subseteq B_0 := \{v := \frac{a}{b^2} j - 2 \mid j \in \mathbb{N},\ v > 0\}.$$

The number of the elements in B_0 which are smaller than $N \in \mathbb{N}$ is bounded by $\frac{N+2}{\frac{a}{b^2}} = (N+2)\frac{b^2}{a}$.

Analogously we get for every $n \in \mathbb{N}$ and $N \in \mathbb{N}$ and $B_n = \{v := \left(\frac{a}{b^2}\right)^{2^n} j - 2 \mid j \in \mathbb{N},\ v > 0\}$

$$\#\{w \in S_n \mid w \leq N\} \leq \#\{v \in B_n \mid v \leq N\} \leq (N+2)\left(\frac{b^2}{a}\right)^{2^n}.$$

Hence

$$\#\{w \in \bigcup_{n=0}^{\infty} S_n \mid w \leq N\} \leq \#\{v \in \bigcup_{n=0}^{\infty} B_n \mid v \leq N\} \leq (N+2)\sum_{n=0}^{\infty}\left(\frac{b^2}{a}\right)^{2^n}.$$

If $a > b^2$ the last sum is convergent and independent of N, i.e.

$$\#\{w \in \bigcup_{n=0}^{\infty} S_n \mid w \leq N\} \leq const(N+2)$$

which means that $\bigcup_{n=0}^{\infty} S_n$ has only linear growth! Thus if $\mathrm{tr}(x)$ is rational the previous argument due to Schmutz is not conclusive: $\mathrm{tr}(x) \in \mathbb{Q}\backslash\mathbb{Z}$ does *not* necessarily imply that $\mathrm{Tr}(Y(x,0,0))$ does not grow linearly! However, we will see in the next section that $\mathrm{tr}(x) \in \mathbb{Q}\backslash\mathbb{Z}$ implies that $\mathrm{Tr}(Y(x,0,0))$ does not satisfy the B-C property.

3.3 $\mathrm{Tr}(Y(x,0,0))$ satisfies the B-C property if and only if $\mathrm{tr}(x)$ is an integer

In this section we prove the main result of the present paper, namely we confirm the first part of Sarnak's Conjecture 1.4:

Theorem 3.4. *Let Γ be a cofinite Fuchsian group with at least one parabolic element. Then $\mathrm{Tr}(\Gamma)$ satisfies the B-C property if and only if Γ is arithmetic.*

Proof. By Theorem 1.3, if Γ is an arithmetic group then $\mathrm{Tr}(\Gamma)$ satisfies the B-C property. So it remains to show that if $\mathrm{Tr}(\Gamma)$ satisfies the B-C property then Γ is an arithmetic Fuchsian group. The proof below follows the ideas of Section 3.1 but instead of the unproven Claim 3.3 we use Proposition 3.6 below.

By Corollary 2.3, for every non-parabolic element T_x in Γ there exists $T_y \in \Gamma$ such that $\langle T_x, T_y\rangle \backslash \mathbb{H}$ contains an Y-piece $Y(x,y,0)$ with $\mathrm{tr}(x) = \mathrm{tr}(T_x)$. If T_x is an elliptic element, then $Y(x,y,0)$ is a degenerated Y-piece. By §3.1 it is enough to show that if $\mathrm{Tr}(\Gamma)$ satisfies the B-C property then, for every $Y(x,y,0)$, $\mathrm{tr}(x)^2$ and $\mathrm{tr}(y)^2$ are integers.

If Γ satisfies the B-C property then, for every Y-piece $Y(x,y,0)$ contained in $\Gamma\backslash\mathbb{H}$, the trace set $\mathrm{Tr}(Y(x,y,0))$ also satisfies the B-C property. Hence it is enough to show that if $\mathrm{Tr}(Y(x,y,0))$ satisfies the B-C property then $\mathrm{tr}(x)^2$ and $\mathrm{tr}(y)^2$ are integers.

If $Y(x,y,0)$ is non-degenerated then the claim follows from the next Proposition 3.5.

If $Y(x,y,0)$ is degenerated, i.e. x corresponds to an elliptic fixed point, then by the remark after Lemma 2.4 the Y-piece $Y(x,y,0)$ contains $Y(\nu_2,y,0)$ and $Y(\nu_3,y,0)$ with $\mathrm{tr}(\nu_2) = 2\mathrm{tr}(x) + \mathrm{tr}(y)$ and $\mathrm{tr}(\nu_3) = 3\mathrm{tr}(x) + 2\mathrm{tr}(y)$. Since $\mathrm{tr}(y) \geq 2$ then $\mathrm{tr}(\nu_2)$ and $\mathrm{tr}(\nu_3)$ are also greater or equal 2. Hence $Y(\nu_2,y,0)$ and $Y(\nu_3,y,0)$ are non-degenerated and by the next Proposition 3.5 it follows that $\mathrm{tr}(\nu_2)^2$, $\mathrm{tr}(\nu_3)^2$ and $\mathrm{tr}(y)^2$ are integers. So $4\mathrm{tr}(x)^2 + 4\mathrm{tr}(x)\mathrm{tr}(y) = \mathrm{tr}(\nu_2)^2 - \mathrm{tr}(y)^2$ and $3\mathrm{tr}(x)^2 + 4\mathrm{tr}(x)\mathrm{tr}(y) = \mathrm{tr}(\nu_3)^2 - \mathrm{tr}(y)^2$ are integers and hence $\mathrm{tr}(x)^2$ is an integer. □

Proposition 3.5. *If $\mathrm{Tr}(Y(x,y,0))$ satisfies the B-C property then $\mathrm{tr}(x)^2$, $\mathrm{tr}(y)^2$ and $\mathrm{tr}(x)\mathrm{tr}(y)$ are integers.*

Proof. The proof is the same as that of Proposition 3.2 but instead of Proposition 3.1 we use Proposition 3.6 below. □

Proposition 3.6. *$\mathrm{Tr}(Y(x,0,0))$ satisfies the B-C property if and only if $\mathrm{tr}(x)$ is an integer.*

In the rest of this Section we are going to prove Proposition 3.6. We will need the following Lemma:

Lemma 3.7. *Let a and b be coprime natural numbers, which are greater than 1. Further let $b = pb_1$, where p is a prime number and $b_1 \in \mathbb{N}$. Then there exist $u, v \in \mathbb{N}\backslash\{0\}$ such that $|ua - vb| = 1$, $v < a$ and $(v,p) = 1$ (and thus also $(v,a) = 1$ and $(u,b) = 1$).*

Proof. Bezout's identity yields $u', v' \in \mathbb{Z}\backslash\{0\}$ such that $u'a + v'b = 1$. We can also write this equivalently as $|\tilde{u}a - \tilde{v}b| = 1$, where $\tilde{u}$ and $\tilde{v}$ are positive natural numbers. Furthermore, we have that $\tilde{v} = qa + r$, where $q, r \in \mathbb{N}$, $r < a$ and $r > 0$, because $(\tilde{v}, a) = 1$ and $a > 1$. Thus after subtracting $0 = q(ba - ab)$ from $|\tilde{u}a - \tilde{v}b|$ we get:

$$|(\tilde{u} - qb)a - rb| = 1.$$

If $(r,p) = 1$ we set $u := \tilde{u} - qb$ and $v := r$. Note that u is positive because a is positive and $rb > 1$.

If $(r,p)=p$ then we subtract $0=ba-ab$ from $(\tilde{u}-qb)a-rb$. We obtain $|(\tilde{u}-(q+1)b)a+(a-r)b|=1$, where $0<a-r<a$ and $(a-r,p)=1$, because $(a,p)=1$ (since p is a divisor of b). From $(a-r)b>1$ and $a>0$ it follows that $\tilde{u}-(q+1)b<0$. We set $u=-(\tilde{u}-(q+1)b)$ and $v=a-r$. $\square$

Proof of Proposition 3.6. If $\mathrm{tr}(x)$ is an integer, then it follows from Proposition 3.1 that $Gap(Y(x,0,0))>0$. This means that in every interval $[n,n+1]$ there are at most $\left[\frac{1}{Gap(Y(x,0,0))}+1\right]$ elements from the set $\mathrm{Tr}(Y(x,0,0))$ and hence $\mathrm{Tr}(Y(x,0,0))$ satisfies the B-C property.

Now let $\mathrm{Tr}(Y(x,0,0))$ satisfy the B-C property. We assume that $\mathrm{tr}(x)$ is *not* an integer. There are two possibilities for $\mathrm{tr}(x)$:

Case 1: $\mathrm{tr}(x)$ is not a rational number.

At the end of Section 3.1 we already showed that in this case $\mathrm{Tr}(Y(x,0,0))$ does not have linear growth and, in particular, does not satisfy the B-C property. Hence Case 1 does not occur.

Case 2: $\mathrm{tr}(x)$ is a rational number (but not an integer).

Then the number $z=\mathrm{tr}(x)+2$ is equal to $\frac{a}{b}$ with a and b coprime natural numbers, $b>1$ and $a>b$ because $z>2$. As in §3.2, it follows from Lemma 2.7 that $\mathrm{Tr}(Y(x,0,0))$ contains $\mathrm{Tr}(Y(x_k,0,0))$ with $\mathrm{tr}(x_k)=z^{2^k}-2$, $k\in\mathbb{N}$. By Lemma 2.4 $\mathrm{Tr}(Y(x_k,0,0))$ contains the set

$$\left\{m(z^{2^k}-2+2)-2 \mid m\in\mathbb{N}\backslash\{0\}\right\}=\left\{m\left(\frac{a}{b}\right)^{2^k}-2 \mid m\in\mathbb{N}\backslash\{0\}\right\}.$$

Claim. *For every $n\in\mathbb{N}$ there exist n different numbers $z_{m_i,k_i}:=m_i\left(\frac{a}{b}\right)^{2^{k_i}}-2$, $i=1,\dots,n$, such that*

$$\max\{z_{m_i,k_i} \mid i=1,\dots,n\}-\min\{z_{m_i,k_i} \mid i=1,\dots,n\}\leq 1.$$

In order to prove this claim we proceed in 5 steps.

Step 1. First we consider a function $f:\mathbb{N}\to\mathbb{N}$ with the following properties: $f(0)=0$ and for $n>0$, $b^{2^{f(n)}}>2\prod_{i=0}^{n-1}a^{2^{f(i)}}$. Such function f exists, because if we assume that we have defined f for $0,\dots,n-1$, then the right-hand side of the inequality is fixed and we can choose $f(n)$ big enough so that the inequality holds. We notice that $f(n+1)>f(n)$ for every $n\in\mathbb{N}$ because

$$b^{2^{f(n+1)}}>2\prod_{i=0}^{n}a^{2^{f(i)}}\geq a^{2^{f(n)}}>b^{2^{f(n)}}.$$

For convenience we set $g(n):=2^{f(n)}$. Then we have $g(0)=1$ and for $n>0$, $b^{g(n)}>2\prod_{i=0}^{n-1}a^{g(i)}$.

Step 2. We fix an arbitrary natural number n greater than 1. Let $b=pb_1$ where p is a prime number and $b_1\in\mathbb{N}$.

Step 3. We can find positive integers u_i,v_i, $i=1,\dots,n$, such that

$$\left|u_i\left(\frac{a}{b}\right)^{g(i)}-v_iv_{i+1}\dots v_n\frac{a}{b}\right|=\frac{a}{b^{g(i)}},$$

where $v_i<a^{g(i)-1}$, $(v_i,a)=1$ and $(v_i,p)=1$. In fact, by Lemma 3.7 there exist $u_n,v_n\in\mathbb{N}\backslash\{0\}$ such that $\left|u_na^{g(n)-1}-v_nb^{g(n)-1}\right|=1$, $v_n<a^{g(n)-1}$, $(v_n,a)=1$ and $(v_n,p)=1$. Hence

$$\left|u_n\left(\frac{a}{b}\right)^{g(n)}-v_n\frac{a}{b}\right|=\frac{a}{b^{g(n)}}\left|u_na^{g(n)-1}-v_nb^{g(n)-1}\right|=\frac{a}{b^{g(n)}}.$$

Since $(a^{g(n-1)-1}, v_n b^{g(n-1)-1}) = 1$, then by Lemma 3.7 there exist $u_{n-1}, v_{n-1} \in \mathbb{N}\backslash\{0\}$ such that $\left|u_{n-1}a^{g(n-1)-1} - v_{n-1}v_n b^{g(n-1)-1}\right| = 1$, where $v_{n-1} < a^{g(n-1)-1}$, $(v_{n-1}, a) = 1$ and $(v_{n-1}, p) = 1$. Hence

$$\left|u_{n-1}\left(\frac{a}{b}\right)^{g(n-1)} - v_{n-1}v_n\frac{a}{b}\right| = \frac{a}{b^{g(n-1)}}\left|u_{n-1}a^{g(n-1)-1} - v_{n-1}v_n b^{g(n-1)-1}\right| = \frac{a}{b^{g(n-1)}}.$$

For $1 \leq i \leq n-1$ we assume that u_j, v_j are defined for all $j = i+1, \ldots, n$. We then define u_i and v_i: Since $(a^{g(i)-1}, v_{i+1}\ldots v_{n-1}v_n b^{g(i)-1}) = 1$, then again by Lemma 3.7 there exist $u_i, v_i \in \mathbb{N}\backslash\{0\}$ such that $\left|u_i a^{g(i)-1} - v_i v_{i+1}\ldots v_{n-1}v_n b^{g(i)-1}\right| = 1$, where $v_i < a^{g(i)-1}$, $(v_i, a) = 1$ and $(v_i, p) = 1$. Hence

$$\left|u_i\left(\frac{a}{b}\right)^{g(i)} - v_i v_{i+1}\ldots v_{n-1}v_n\frac{a}{b}\right| = \frac{a}{b^{g(i)}}\left|u_i a^{g(i)-1} - v_i v_{i+1}\ldots v_{n-1}v_n b^{g(i)-1}\right| = \frac{a}{b^{g(i)}}.$$

Step 4. Set $m_0 := v_1\ldots v_{n-1}v_n$ and $m_i := v_1\ldots v_{i-1}u_i$ for all $i = 1, \ldots, n$. We claim that the numbers $z_{m_i,f(i)} = m_i\left(\frac{a}{b}\right)^{2^{f(i)}} - 2$, $i = 0, \ldots, n$, are all inside an interval of length 1. Indeed, for every $i = 1, \ldots, n$:

$$\begin{aligned}
\left|z_{m_i,f(i)} - z_{m_0,f(0)}\right| &= \left|m_i\left(\frac{a}{b}\right)^{g(i)} - 2 - m_0\left(\frac{a}{b}\right)^{g(0)} + 2\right| \\
&= v_1\ldots v_{i-1}\left|u_i\left(\frac{a}{b}\right)^{g(i)} - v_i\ldots v_n\frac{a}{b}\right| = v_1\ldots v_{i-1}\frac{a}{b^{g(i)}} \\
&< \frac{a^{g(1)-1}\ldots a^{g(i-1)-1}a}{b^{g(i)}} \leq \frac{\prod_{j=0}^{i-1}a^{g(j)}}{b^{g(i)}} < \frac{1}{2},
\end{aligned}$$

where the last inequality follows from our choice of the function g.

Step 5. We finally show that the numbers $z_{m_i,f(i)}$, $i = 0, \ldots, n$ are all different.

For every $i = 1, \ldots, n$, u_i satisfies $(u_i, p) = 1$, because $(u_i, b) = 1$ (otherwise the difference $\left|u_i a^{g(i)-1} - v_i\ldots v_n b^{g(i)-1}\right|$ could not be equal to 1). We have chosen v_i, $i = 1, \ldots, n$, such that $(v_i, p) = 1$. Hence p does not divide $m_i = v_1\ldots v_{i-1}u_i$ and $m_0 = v_1\ldots v_{n-1}v_n$. Note also that $(p, a) = 1$.

Let d be the exponent of p in the prime number decomposition of b. Write $z_{m_i,f(i)} = m_i\left(\frac{a}{b}\right)^{2^{f(i)}} - 2 = \frac{s}{t}$, with $s, t \in \mathbb{N}\backslash\{0\}$, $(s, t) = 1$. Then $p^{d2^{f(i)}}$ divides t and $p^{d2^{f(i)}+1}$ does not divide t. Hence, since for $i \neq j$, $f(i) \neq f(j)$, the numbers $z_{m_i,f(i)}$ and $z_{m_j,f(j)}$ are different.

This completes the proof of the claim, which in turn implies that $\mathrm{Tr}(Y(x, 0, 0))$ does not satisfy the B-C property and we have a contradiction also in Case 2. This completes the proof of Proposition 3.6. □

3.4 Final remarks

In spite of the gap, Theorem 9 in [6] remains true: A cofinite Fuchsian group Γ containing parabolic elements is arithmetic if and only if, for every Y-piece $Y(x, 0, 0)$ that is contained in $\Gamma\backslash\mathbb{H}$, $\mathrm{tr}(x)$ is an integer.

On the other hand, it is not clear yet if Theorem 10 and Corollary 4 in [6] are also true, i.e. that the trace set of a non-arithmetic Fuchsian group grows faster than the trace set of any arithmetic Fuchsian group. By Theorem 1.3 the trace set of an arithmetic Fuchsian group satisfies the B-C property and hence grows linearly. But it is an open question if there is a non-arithmetic Fuchsian group whose trace set also grows linearly.

References

[1] P. Buser, *Geometry and spectra of compact Riemann Surfaces*, Birkhäuser Boston Inc., Boston, 1992.

[2] S. Katok, *Fuchsian Groups*, Chicago Lectures in Math., University of Chicago Press, Chicago, 1992.

[3] W. Luo and P. Sarnak, *Number variance for arithmetic hyperbolic surfaces*, Comm. Math. Phys. **161** (1994), 419-432.

[4] C. Maclachlan and A. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Mathematics **219**, Springer-Verlag, 2003.

[5] P. Sarnak, *Arithmetic quantum chaos*, Israel Math. Conf. Proc. **8** (1995), 183-236.

[6] P. Schmutz, *Arithmetic groups and the length spectrum of Riemann surfaces*, Duke Math. J. **84** (1996), 199-215.

[7] K. Takeuchi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), 600-612.