The arithmetic and geometry of Salem numbers

Eknath Ghate
and
Eriko Hironaka

August 15, 2000

Abstract

A Salem number is a real algebraic integer, greater than 1, with the property that all of its conjugates lie on or within the unit circle, and at least one conjugate lies on the unit circle. In this paper we survey some of the recent appearances of Salem numbers in parts of geometry and arithmetic, and discuss the possible implications for the 'minimization problem'. This is an old question in number theory which asks whether the set of Salem numbers is bounded away from 1.

A.M.S. Classification: 11R06, 11R52, 20F32

Contents

1 Introduction

A *Salem number* is a real algebraic integer, greater than 1, with the property that all its conjugates lie on or within the unit circle, and at least one conjugate lies on the unit circle. This paper deals with the following unsolved problem:

Problem 1 (Minimization problem) *Is the set of Salem numbers bounded away from* 1*?*

The minimization problem is closely related to the following question posed by Lehmer [25] in 1933.

Problem 2 (Lehmer's question) *Is there a* $\delta > 0$ *such that the Mahler measure of every irreducible monic polynomial* $P(x)$ *with integer coefficients is either 1 or larger than* $1 + \delta$*?*

The *Mahler measure* $M(P)$ of a monic polynomial $P(x) \in \mathbb{Z}[x]$ is the product of the absolute values of the roots of $P(x)$ which lie outside the unit circle, and is 1 if there are no such roots:

$$M(P) = \prod_{P(\theta)=0} \max\{1, |\theta|\}.$$

Thus $M(P) \geq 1$ and it may be checked that if $P(x)$ is irreducible then $M(P) = 1$ if and only if $P(x)$ is a cyclotomic polynomial or the monomial x.

Of special interest to Lehmer were *palindromic* polynomials (also sometimes called *reciprocal* or *symmetric* polynomials): these are polynomials $P(x) \in \mathbb{Z}[x]$ that satisfy

$$P(x) = x^m P(1/x),$$

where m is the degree of $P(x)$. Equivalently, palindromic polynomials are integer polynomials that read the same whether read backwards or forwards. For any palindromic polynomial, if α is a root, then so is $1/\alpha$. Hence, a nonlinear, palindromic polynomial must have even degree since palindromic polynomials of odd degree always have -1 as a root. In [25], Lehmer found the monic palindromic polynomials of degrees 2, 4, 6, and 8 with smallest Mahler measure. For degree 10 and higher, the best polynomial Lehmer could find was

$$L(x) \ = \ x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1, \tag{1}$$

which we will refer to throughout this paper as the *Lehmer polynomial.* This polynomial still stands today as the monic polynomial with smallest known Mahler measure:

$$M(L) = 1.17628\ldots$$

If $P(x) \in \mathbb{Z}[x]$ is a monic, irreducible polynomial with $M(P) < M(L)$, then $P(X)$ must be palindromic, since Smyth has shown [40] that $1.32471\ldots$, the unique real root of $S(x) = x^3 - x - 1$, is a lower bound for the set of Mahler measures of non-palindromic polynomials with Mahler measure strictly larger than 1.

We will refer to the minimal polynomial of a Salem number ϵ as a *Salem polynomial.* Its Mahler measure is clearly just ϵ. It is not difficult to prove that Salem polynomials are always palindromic.

The Lehmer polynomial $L(x)$ is a Salem polynomial: it is the minimal polynomial of the Salem number $\epsilon_L = 1.17628\cdots = M(L)$. Thus ϵ_L is both the smallest known Salem number, and the smallest known Mahler measure.

Flammang, Grandcolas, and Rhin [18] have shown that there are no Salem numbers less than 1.3, of degree less than 40, other than the forty-seven Salem numbers tabulated by Boyd and Mossinghoff in [5], [6] and [29]. As a consequence, if there is a Salem number smaller than ϵ_L, it would have to have degree larger than 40.

The purpose of this note is to expose some of the recent appearances that Salem numbers, and more generally Mahler measures, have made in arithmetic and geometry. A more detailed overview of the topics we treat is given in the next Section. We have tried to adopt an interdisciplinary viewpoint which we hope will shed a fresh perspective on the minimization problem.

In closing this Introduction we mention that Salem numbers originally arose in the study of Fourier analysis and uniform distribution [34]. The reader can find a convenient survey of some properties of Salem numbers and those of the closely related Pisot-Vijayaraghavan numbers in [8] and [2]. Here too the reader will find a more detailed discussion of certain aspects of the minimization problem. Another area related to Mahler measures, which we do not touch upon, is the field of dynamical systems. The jumping off point here is that the entropy of certain dynamical systems attached to polynomials equals the logarithm of the Mahler measure of these polynomials. We simply refer the curious reader to the works [26], [35], [17], and [39] for further details.

Acknowledgments We would like to thank D. Boyd, D. Lind, C. McMullen, M. Mossinghoff, P. Sarnak, J.-P. Serre, B. Sury, D. Ulmer, and T. N. Venkataramana for useful conversations and correspondence, and the members and staff of the I.H.E.S. where the research for this paper began. We are also indebted to the referee for helpful comments.

2 Overview of the paper

Here is a brief overview of the contents of this paper.

Sections 3.1 to 3.4 describe a relation between the minimization problem for Salem numbers and a minimization problem for the lengths of closed geodesics on arithmetic hyperbolic surfaces, i.e., hyperbolic surfaces attached to arithmetic Fuchsian groups. This material was worked out by the authors, but it is certainly not new (see, for example, Neumann and Reid [30]). An equivalent formulation of these ideas in terms of lattices in semi-simple real Lie groups was first worked out by Sury in [45]. We recall this briefly in Section 3.5.

Floyd and Plotnick [19] showed that some Salem numbers, including ϵ_L above, are equal to the asymptotic growth rates of certain hyperbolic planar reflection groups. The smallest Salem number that arises in this way is again ϵ_L, as shown by the second author in [22]. These matters are described in Section 4.1.

The role of Alexander polynomials in the study of Salem numbers and the minimization problem is discussed in Section 4.3. The second author has shown [22] that the Salem polynomials arising, as in Section 4.1, from polygonal reflection groups, are the Alexander polynomials of certain pretzel knots. A corollary is that Lehmer's polynomials solves the minimization problem for this family of polynomials.

In Section 5 we explain how Salem numbers and Mahler measures show up in the special values of L-functions. We start, in Section 5.1, with an observation of Chinburg [12], who relates Salem numbers to Stark units, and hence to the values of certain (abelian) Artin L-functions at $s = 0$. Then, in Section 5.2, we describe work and conjectures of Costa, Friedman and Skoruppa [21] on the ratios of regulators of extensions of number fields, and its relation to the minimization problem.

Pursuing this theme further, we discuss, in Section 5.3, some recent striking results of Smyth, Ray, Boyd, Deninger, Bornhorn and Rodriguez Villegas, that show that the special values of more general L-functions are connected to the logarithms of Mahler measures of polynomials in many variables. The possible implications for the minimization problem are discussed following Boyd in [9].

We conclude in Section 6 with a review of some of the sharpest results known to us in the direction of solving the minimization problem. These results have been obtained by methods completely different from those described in this paper. We also refer the reader to the web page on Lehmer's Conjecture maintained by Mossinghoff [28] where, among other things, much up to date numerical information related to Lehmer's question may be found.

3 Geodesics on arithmetic hyperbolic surfaces

In this section we show that the minimization problem for Salem numbers is equivalent to the minimization problem for the lengths of closed geodesics on arithmetic hyperbolic surfaces.

3.1 Salem extensions

We start by describing some properties of the number field $L = \mathbb{Q}(\epsilon)$ generated by a Salem number ϵ.

A *number field* L is a field extension of $\mathbb{Q}$ of finite degree over $\mathbb{Q}$. We may write $L = \mathbb{Q}(\theta)$ for an element $\theta \in L$ which generates L over $\mathbb{Q}$. Consequently we may identify L with $\mathbb{Q}[x]/\langle P(x) \rangle$, where $P(x) \in \mathbb{Z}[x]$ is the minimal polynomial of θ. Then the *degree* of L is the dimension of L as a vector space over $\mathbb{Q}$, and equals the degree of the minimal polynomial $P(x)$.

If ω is any root of $P(x)$ (ω is called a *conjugate* of θ), then there is a unique isomorphism from L to $\mathbb{Q}(\omega)$ sending x to ω. Thus, each root ω of $P(x)$ defines a $\mathbb{Q}$-algebra monomorphism

$$\sigma_\omega : L \xrightarrow{\simeq} \mathbb{Q}(\omega) \subset \mathbb{C}.$$

Composition by complex conjugation yields another (possibly identical) embedding

$$\overline{\sigma_\omega} \quad (= \sigma_{\overline{\omega}})\,.$$

A pair of such embeddings $\{\sigma, \overline{\sigma}\}$ is called an *infinite place* of L. An infinite place is *real* if $\sigma = \overline{\sigma}$, otherwise it is *complex*. In the former case we set $L_\sigma = \mathbb{R}$, and in the latter case we set $L_\sigma = \mathbb{C}$, and call L_σ the completion of L at the place σ. If all the infinite places of L are real, then we say L is a *totally real* number field.

Since $\mathbb{C}$ and $\mathbb{R}$ have natural topologies, each of the infinite places of L induce (distinct) topologies on L. However there are other topologies on L, the *non-archimedean* topologies. The natural embeddings of L into the $\mathfrak{q}$-adic completions of L, as $\mathfrak{q}$ varies through the prime ideals of L,

$$\sigma_{\mathfrak{q}} : L \to L_{\mathfrak{q}},$$

induce such topologies on L. For this reason, we will refer to the primes $\mathfrak{q}$, and sometimes even to the corresponding embeddings $\sigma_{\mathfrak{q}}$, as the *finite places* of L.

Now let ϵ be a Salem number, i.e., an algebraic integer all of whose conjugates like on or inside the unit circle with at least one on the unit circle, and let $K = \mathbb{Q}(\epsilon)$ be the number field generated by ϵ. We identify K with $\mathbb{Q}[x]/\langle P(x)\rangle$ where $P(x)$ is the minimal polynomial of ϵ. As mentioned already in the Introduction, the degree of K must be even, since $P(x)$ is irreducible and palindromic. Say this degree is $2n$.

Note that all the conjugates of ϵ, except for $\frac{1}{\epsilon}$, which is also real, lie *on* the unit circle. This is because if any complex root z of $P(x)$ were to lie strictly within the unit circle, then the root $\frac{1}{z}$ would lie outside it, contradicting the definition of ϵ. Thus a list of the conjugates of ϵ can be written as

$$\epsilon, \frac{1}{\epsilon}, z_1, \overline{z_1}, \ldots, z_{n-1}, \overline{z_{n-1}},$$

where $|z_i| = 1$, for $i = 1, \ldots, n-1$. A plot of the set of conjugates of a typical Salem number ϵ is given in Figure 3.1.

By the general discussion above we see that K has $n-1$ complex places, say $\tau_1, \ldots, \tau_{n-1}$, corresponding to the roots $z_1, \ldots, z_{n-1}$, and two real places, say τ and τ', corresponding to ϵ and $1/\epsilon$ respectively.

Since $P(x)$ is monic, irreducible, and palindromic, of degree at least 4 (recall that a Salem number has at least one conjugate on the unit circle) we may further write

$$P(x) = x^n Q\left(x + \frac{1}{x}\right),$$

for some monic, irreducible polynomial $Q(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$. We see that $Q(x)$ has n real roots, namely $\alpha = \epsilon + \frac{1}{\epsilon}$, and $\alpha_i = z_i + \overline{z_i}$, for $i = 1, \ldots, n-1$.

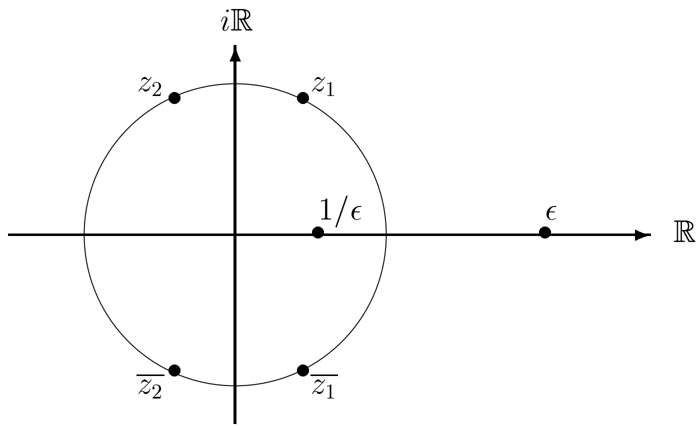

Figure 1: A (degree six) Salem number ϵ and its conjugates

Set $k = \mathbb{Q}(\alpha)$, where $\alpha = \epsilon + \frac{1}{\epsilon}$ is the unique (real) root of $Q(x)$ larger than 2. Thus, k is a number field of degree n. We will call the quadratic field extension K/k a *Salem extension.*

Note that k is a totally real field. Let σ denote the real place of k corresponding to α, and let $\sigma_1, \ldots, \sigma_{n-1}$ denote the other real places of k, corresponding to $\alpha_1, \ldots, \alpha_{n-1}$.

The places of K and k are related. Namely τ and τ' *lie over* the place σ of k. This means that $\sigma(k) \subset \tau(K)$ and $\sigma(k) \subset \tau'(K)$. Similarly the places $\tau_1, \ldots, \tau_{n-1}$ of K lie over the places $\sigma_1, \ldots, \sigma_{n-1}$ of k.

Note that ϵ is a root of the polynomial

$$f(x) = x^2 - \alpha x + 1.$$

Conversely, for any real algebraic integer $a > 2$ (of degree larger than 2) whose conjugates are all real and lie in $(-2, 2)$, the root e larger than 1 of the polynomial

$$f(x) = x^2 - ax + 1,$$

is a Salem number.

Now let L be an arbitrary totally real field of degree $d \geq 2$ over $\mathbb{Q}$. We say that a Salem number ϵ is a *Salem number over* L if the totally real field $k = \mathbb{Q}(\epsilon + 1/\epsilon)$ equals L. Let $\mathcal{S}(L)$ denote the set of all Salem numbers over L.

Let ι be a real place of L. If, in addition, the embedding σ of k coincides with the embedding ι of L, then we say ϵ is a Salem number over L *of type* ι. Let $\mathcal{S}(L, \iota)$ denote the set of all Salem numbers over L of type ι. Clearly we have $\mathcal{S}(L) = \bigcup_\iota \mathcal{S}(L, \iota)$, as ι varies through all the infinite places of L. Now let, for $d \geq 2$,

$$\mathcal{S}_d = \bigcup_L \mathcal{S}(L),$$

where L runs over all totally real fields of degree d. Thus $\mathcal{S}_d$ is the set of all Salem numbers of degree $2d$. We have the following easy Lemma.

Lemma 3 *The set $\mathcal{S}_d$ has a minimal element.*

Proof. We show more generally that the set of Mahler measures of monic polynomials of degree $2d$ is a discrete set, and therefore has a minimal element. Let $P(x) = \sum_{r=0}^{2d} a_{2d-r}x^r \in \mathbb{Z}[x]$ denote such a polynomial. Since a_r is, up to sign, a sum of the products of the roots of $P(x)$ chosen r at a time, we see that

$$|a_r| \leq \binom{2d}{r} \cdot M(P).$$

Consequently, there are only finitely many monic polynomials of degree $2d$ with bounded Mahler measure. The Lemma follows.

■

3.2 Arithmetic Fuchsian groups

A group Γ is a *Fuchsian group of the first kind* if Γ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ and the quotient $\Gamma\backslash H$ of the upper half plane H by Γ has finite volume.

An *arithmetic Fuchsian group* is a Fuchsian group of the first kind which can be constructed out of a totally real number field in a manner that we shall describe in this section. More detailed treatments can be found in [37] and [49].

Let L be any number field. A *central simple quaternion algebra over L* is an associative L-algebra D with unit such that

- the center of D is L,
- the only two sided ideals of D are the trivial ideal and D itself, and,
- the dimension of D over L is 4.

It is a consequence of a general theorem of Wedderburn [23], that any such algebra is either a *division algebra* (that is, D has no zero divisors), or that D is isomorphic to $\mathrm{M}_2(L)$, the algebra of 2 by 2 matrices over L.

D can be equipped with the *reduced trace* and *reduced norm* maps:

$$\mathrm{red\,Tr} : D \to L, \quad \text{and}, \quad \mathrm{red\,Nm} : D^\times \to L^\times,$$

defined as follows. Fix an extension F of L that *splits* D. This means there is an isomorphism

$$h : D \otimes_L F \ \stackrel{\sim}{\to}\ \mathrm{M}_2(F).$$

Such an F always exists. Now define

$$\operatorname{red}\operatorname{Tr}(x) = \operatorname{trace} h(x) \;\text{ and }\; \operatorname{red}\operatorname{Nm}(x) = \det h(x).$$

One checks that, so defined, red Tr and red Nm take values in $L \subset F$, and that their definition is independent of the choice of F and h.

We say that D is *unramified* or *split* at a place

$$\sigma : L \hookrightarrow L_\sigma$$

of L, which may be either finite or infinite, if the tensor product,

$$D \otimes_{L,\sigma} L_\sigma,$$

viewed as a central simple quaternion algebra over L_σ, is isomorphic to $\mathrm{M}_2(L_\sigma)$. Otherwise $D \otimes_{L,\sigma} L_\sigma$ is a division algebra, and in this case, we say that D is *ramified* at σ.

If σ is a complex place, then D is necessarily split at σ. If σ is a real place, then D may ramify at σ, in which case

$$D \otimes_{L,\sigma} \mathbb{R} \simeq \mathbb{H}$$

is the usual Hamilton algebra of quaternions over $\mathbb{R}$.

An important property of the quaternion algebras D in this context is that every such D is ramified at an *even* number of non-complex places. Conversely, for any finite collection Σ of non-complex places of L, of even cardinality, there is a *unique* (up to isomorphism) central simple quaternion algebra D over L which is ramified at exactly the places in Σ. In particular, if D is unramified everywhere ($\Sigma = \emptyset$), then D is isomorphic to $\mathrm{M}_2(L)$.

Remark. Much of the above discussion can be described very elegantly by the following exact sequence from class field theory (see for example [38], Chapter 10 or [1]):

$$0 \to \mathrm{Br}(L) \to \bigoplus_\sigma \mathrm{Br}(L_\sigma) \to \mathbb{Q}/\mathbb{Z} \to 0, \tag{2}$$

where the sum runs over all places σ, both finite and infinite, of L. Here $\mathrm{Br}(L)$, respectively $\mathrm{Br}(L_\sigma)$, denotes the Brauer group of L, respectively of L_σ. We make this remark simply to orient the more knowledgeable reader. In essence all the information contained in (2) that we shall need in the sequel has already been discussed above in words.

Now suppose that L is totally real, with infinite places $\iota_1, \dots, \iota_d$. Fix a place ι ($= \iota_j$ for some $j = 1, \dots, d$) of L. We would like to impose the following condition on the 'ramification of D at ∞'. We assume that D is unramified at a single infinite place ι and ramified at all other infinite places. That is, we assume that

$$D \otimes_{\mathbb{Q}} \mathbb{R} \;=\; \bigoplus_{r=1}^{d} D \otimes_{L,\iota_r} \mathbb{R} \;=\; \mathbb{H} \oplus \cdots \oplus \mathbb{H} \oplus \mathrm{M}_2(\mathbb{R}) \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}, \quad (3)$$

with the single summand $\mathrm{M}_2(\mathbb{R})$ corresponding to the place ι, and $d-1$ copies of the Hamilton algebra $\mathbb{H}$ corresponding to the other places.

An *order* $\mathcal{O}$ in D is a subring of D such that

- $\mathcal{O}$ contains the ring $\mathcal{O}_L$ of integers of L, and,
- $\mathcal{O} \otimes_{\mathcal{O}_L} L = D$.

A *maximal order* is an order which is not properly contained in any other. Let $\mathcal{O}$ be a maximal order in D and let U be the set of unit elements of $\mathcal{O}$ of reduced norm one.

When L is totally real, and D has ramification at ∞ given by (3), we let $\Gamma(D,\mathcal{O},\iota) \subset \mathrm{SL}_2(\mathbb{R})$ be the image of U under the embedding ι fixed above. It turns out that $\Gamma(D,\mathcal{O},\iota)$ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$, and that the volume of the quotient surface $\Gamma(D,\mathcal{O},\iota)\backslash H$ is finite. Thus $\Gamma(D,\mathcal{O},\iota)$ is a Fuchsian group of the first kind. If the defining field L is not equal to $\mathbb{Q}$, then the quotient surface is also compact.

A Fuchsian group of the first kind of the form $\Gamma(D,\mathcal{O},\iota)$ is called an *arithmetic Fuchsian group*. The corresponding quotient surface $\Gamma(D,\mathcal{O},\iota)\backslash H$ is called an *arithmetic hyperbolic surface*. In the following sections, we will primarily be interested in *cocompact* arithemetic Fuchsian groups. These are arithmetic Fuchsian groups whose corresponding quotient surface is compact. A Fuchsian group of the form $\Gamma(D,\mathcal{O},\iota)$ is cocompact as long as it is defined over a totally real number field not equal to $\mathbb{Q}$, i.e., of degree greater than or equal to 2.

Up to conjugation in $\mathrm{SL}_2(\mathbb{R})$, $\Gamma(D,\mathcal{O},\iota)$ does not depend on the choice of $\mathcal{O}$. Indeed although there is more than one maximal order in D, since D is split at one infinite place, all its maximal orders are conjugate to each other, and hence the corresponding Fuchsian group is determined up to inner automorphism of $\mathrm{SL}_2(\mathbb{R})$.

In view of the remarks at the beginning of this section, if the degree d of L is odd, there is a unique D (up to isomorphism over L) which is unramified at all the finite places, and is ramified at all infinite places except at ι. We will denote this D by D_ϕ. On the other hand, if d is even, then a choice of a finite place p of L will again give a canonical choice of D (up to isomorphism), which is unramified at all the finite places except p and ramified at all the infinite places except ι. We shall denote this D by D_p, to show that it depends on the prime p of L. The corresponding arithmetic Fuchsian groups are denoted by $\Gamma(D_\phi,\mathcal{O},\iota)$ and $\Gamma(D_p,\mathcal{O},\iota)$ respectively.

3.3 Salem numbers and hyperbolic matrices

In this section we show how Salem numbers are closely related to the eigenvalues of hyperbolic elements in cocompact arithmetic Fuchsian groups.

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be an arbitrary Fuchsian group of the first kind. An element $\gamma \in \Gamma$ is said to be *hyperbolic* if its eigenvalues are distinct and real. Let $f_\gamma(x)$ be the characteristic polynomial of γ. Then since $\det(\gamma) = 1$, we have

$$f_\gamma(x) = x^2 - \mathrm{tr}(\gamma)x + 1.$$

Thus, γ is hyperbolic if and only if $|\mathrm{tr}(\gamma)| > 2$. Moreover, in this case the roots of $f_\gamma(x)$ form a pair of positive real reciprocal numbers. Let $\epsilon(\gamma)$ be the root which is larger than 1, and let

$$N(\gamma) = \epsilon(\gamma)^2$$

be the *norm* of $\gamma \in \Gamma$.

Proposition 4 *Let $\Gamma = \Gamma(D, \mathcal{O}, \iota)$ be an arithmetic Fuchsian group. If $\gamma = \iota(u) \in \Gamma(D, \mathcal{O}, \iota)$ is not equal to the identity or its negative, then the conjugates of* $\mathrm{trace}(u)$ *in L lie in the interval* $(-2, 2)$.

Proof. By construction (see Section 3.2) the conjugates $\iota'(u)$ of u (for $\iota' \neq \iota$) lie in the group of norm one units of the Hamilton quaternion algebra over $\mathbb{R}$. Thus, they are of the form

$$\iota'(u) = a + bi + cj + dk,$$

with a, b, c and $d \in \mathbb{R}$, and with

$$\mathrm{norm}(\iota'(u)) = a^2 + b^2 + c^2 + d^2 = 1.$$

Since a is real, we see that $|a| \leq 1$, and hence $|\iota'(\mathrm{red\,Tr}(u))| = |\mathrm{trace}(\iota'(u))| = |2a| \leq 2$. If $|a| = 1$, we have $\iota'(u) = \pm 1$, and hence u, and therefore γ, is either the identity or its negative. The proposition follows.

■

Proposition 5 *Let $\Gamma = \Gamma(D, \mathcal{O}, \iota)$ be a cocompact arithmetic Fuchsian group, and let $\gamma \in \Gamma$ be a hyperbolic element. Then $\epsilon(\gamma)$ is a Salem number.*

Remark. In fact we show that $\epsilon(\gamma)$ is the image of a Salem number ϵ under the unique real infinite place of $\mathbb{Q}(\epsilon)$ which realizes ϵ as a real number larger than 1. Thus here, and sometimes in the sequel, we identify a Salem number with its image under such an embedding.

Proof. Assume that $\gamma = \iota(u)$. By Proposition 4 above, $\alpha = \mathrm{red}\,\mathrm{Tr}(u)$ is an integer in L, with $\iota(\alpha) > 2$, and with all other conjugates lying in $(-2, 2)$. Thus, since $\epsilon(\gamma)$ is the larger root of

$$f_\gamma(x) = x^2 - \iota(\alpha)x + 1,$$

$\epsilon(\gamma)$ is a Salem number.

■

Let L be a totally real number field of degree greater than or equal to 2. Let us define $\mathcal{S}(\Gamma(D, \mathcal{O}, \iota))$ to be the set of those Salem numbers ϵ satisfying:

- ϵ is the larger eigenvalue of a hyperbolic element in $\Gamma(D, \mathcal{O}, \iota)$, and,
- the degree of ϵ is $2d$, that is, $\alpha = \epsilon + 1/\epsilon$ generates L.

Note that the set $\mathcal{S}(\Gamma(D, \mathcal{O}, \iota))$ does not depend on the choice of the maximal order $\mathcal{O}$.

In Section 3.1 we had defined $\mathcal{S}(L, \iota)$ as the set of all Salem numbers over L of type ι. Proposition 5 shows that

$$\mathcal{S}(\Gamma(D, \mathcal{O}, \iota)) \subset \mathcal{S}(L, \iota).$$

We now ask whether it is possible to capture the entire set $\mathcal{S}(L, \iota)$ by *one* division algebra. When the degree d of L is odd, this is indeed possible:

Proposition 6 *Assume that d is odd, and that D_ϕ is defined as in the end of Section 3.2. Then*

$$\mathcal{S}(L, \iota) = \mathcal{S}(\Gamma(D_\phi, \mathcal{O}, \iota)).$$

Proof. One containment has been shown. To show the other, let $\epsilon \in \mathcal{S}(L, \iota)$. Let K/k be the corresponding Salem extension (see Section 3.1 for the definition of a Salem extension, and for notation that we shall use below). We have $k = L$, $n = d$, and $\sigma = \iota$. We claim that K is isomorphic to a maximal subfield of D_ϕ. A general theorem about division algebras shows that it suffices to check that K splits D_ϕ. By the remarks in Section 3.2 applied to K, we see that it is enough to check that each completion $K_\wp$ of K (finite or infinite) splits $D_\phi \otimes_k K$. But

$$D_\phi \otimes_k K \otimes_K K_\wp = D_\phi \otimes_k k_p \otimes_{k_p} K_\wp,$$

where $p = \wp \cap \mathcal{O}_k$ is the prime of k lying under the prime $\wp$ of K. By hypothesis, D_ϕ is already split by k_p for finite p, so there is nothing to check at the finite places. At the infinite places, a similar phenomena occurs at σ. As for the other infinite places σ_i ($i = 1, \dots, n-1$), we just note that the Hamilton algebra is split by the complex numbers.

Thus, K splits D_ϕ, and so the Salem extension K/k sits inside D. Since the Salem number ϵ generates K, it gives an element $\gamma_\epsilon \in \Gamma(D_\phi, \mathcal{O}, \iota)$, for some maximal order $\mathcal{O} \subset D$. Note that γ_ϵ is hyperbolic, since its trace is just $\sigma(\mathrm{tr}_{K/k}(\epsilon)) = \sigma(\epsilon + \frac{1}{\epsilon}) = \sigma(\alpha) > 2$. Clearly the larger eigenvalue $\epsilon(\gamma_\epsilon)$ of γ_ϵ is just $\tau(\epsilon)$. Finally the degree of ϵ is $2d$. This shows the other inclusion.

■

When the degree d of L is even, $\mathcal{S}(L, \iota)$ may not be equal to $\mathcal{S}(\Gamma(D, \mathcal{O}, \iota))$ for one particular D. First we introduce some terminology. Let K/k be an arbitrary quadratic extension of number fields. A prime ideal p of k is said to be *inert* in K if the ideal $\wp$ generated by p in $\mathcal{O}_K$ is a prime ideal of K. Also, p is said to *split* in K if the ideal generated by p in $\mathcal{O}_K$ factors as a product of two distinct prime ideals of K.

Let us now assume that $\epsilon \in \mathcal{S}(L, \iota)$. Let K/k denote the Salem extension corresponding to ϵ. Fix a division algebra D over L with ramification as in (3). Let $\Sigma_f(D)$ denote the set of finite places of D where D is ramified. Recall that $\Sigma_f(D)$ is a finite set of odd cardinality. The following proposition gives a criterion to check whether ϵ is the (larger) eigenvalue of a hyperbolic matrix in $\Gamma(D, \mathcal{O}, \iota)$.

Proposition 7 *Assume that d is even.*

1. *If for each $p \in \Sigma_f(D)$, p is inert in K, then K sits inside D.*
2. *If K sits inside D, then for all $p \in \Sigma_f(D)$, p does not split in K.*

Proof. The proof of the first statement of Proposition 7 is exactly the same as the proof of Proposition 6, except that, additionally, for each $p \in \Sigma_f$, we have to check the splitting of $D_p \otimes_k K$ at $K_\wp$, where $\wp$ is the prime of K generated by p. But since

$$D_p \otimes_k K \otimes_K K_\wp = D_p \otimes_k k_p \otimes_{k_p} K_\wp,$$

it suffices to show that the extension $K_\wp / k_p$ splits $D_p \otimes_k k_p$. But this follows from the general fact that over a local field, a quaternion algebra is always split by the unique unramified extension of degree 2 (see [38], Chapter 12).

For the second statement, fix $p \in \Sigma_f$. If $p = \wp\wp'$ splits in K and K sits in D, then $D \otimes_k k_p$ would contain the subalgebra $K \otimes_k k_p = K_\wp \times K_{\wp'}$ which has zero divisors. This is a contradiction.

■

Proposition 7 shows that, when the degree d of L is even, we may not be able to find a single, or even finitely many, division algebras D which account for all Salem numbers over L (of type ι). We must be content with the following result:

Corollary 8 *Assume d is even, and let D_p be the division algebra over L defined as in the end of Section 3.2. Then*

$$\mathcal{S}(L,\iota)=\bigcup_{p}\mathcal{S}(\Gamma(D_p,\mathcal{O},\iota))=\bigcup_{D}\mathcal{S}(\Gamma(D,\mathcal{O},\iota)),$$

where p varies through all finite places of L, and D varies over all division algebras over L that are ramified at exactly one infinite place.

Proof. Let $\epsilon \in \mathcal{S}(L,\iota)$, and let K/k denote the corresponding Salem extension. Choose a prime p of k such that p is inert in K. Then, by Proposition 7, $\epsilon \in \mathcal{S}(\Gamma(D_p,\mathcal{O},\iota))$. All the other containments have already been shown or are obvious.

■

3.4 Closed geodesics on hyperbolic surfaces

In this section we discuss the geometry of arithmetic surfaces, and describe a bijection between conjugacy classes of hyperbolic elements in arithmetic Fuchsian groups Γ, and closed geodesics on the quotient surface $\Gamma\backslash H$. In the next section we will apply this to the cocompact arithmetic Fuchsian groups $\Gamma=\Gamma(D,\mathcal{O},\iota)$.

Let $\Gamma\subset \mathrm{SL}_2(\mathbb{R})$ be an arbitrary Fuchsian group of the first kind. Recall that a matrix $\gamma\in\Gamma$ hyperbolic if and only if $|\mathrm{tr}(\gamma)|>2$. We say that a matrix $\gamma\in\Gamma$ is *elliptic*, respectively *parabolic*, if $|\mathrm{tr}(\gamma)|<2$, respectively $|\mathrm{tr}(\gamma)|=2$. As a transformation of $\mathbb{C}\cup\infty$, γ has the following properties (see [49], page 115):

$$\begin{aligned}
\gamma \text{ is hyperbolic} \quad &\Longleftrightarrow \quad \gamma \text{ has two distinct fixed points in } \mathbb{R}\cup\infty,\\
\gamma \text{ is elliptic} \quad &\Longleftrightarrow \quad \begin{cases} \gamma \text{ has two distinct fixed points of the form} \\ \qquad\qquad z,\overline{z},\ \text{ for } z\in\mathbb{C},\ \text{ and,}\end{cases}\\
\gamma \text{ is parabolic} \quad &\Longleftrightarrow \quad \gamma \text{ has a unique fixed point in } \mathbb{R}\cup\infty.
\end{aligned}$$

The Fuchsian group Γ is cocompact if Γ does not have any parabolic elements. If Γ does not have any elliptic elements, then $\Gamma\backslash H$ is smooth, i.e., a Riemann surface. Otherwise, it is an *orbifold*, with singularities corresponding to the fixed points, called *elliptic points*, of elliptic elements.

Proposition 9 *Let Γ be any Fuchsian group. Then there is a bijection between conjugacy classes of hyperbolic elements $\gamma \in \Gamma$ and closed geodesics $g(\gamma)$ on $\Gamma\backslash H$. In this correspondence, the length of $g(\gamma)$ is $\log N(\gamma)$.*

Proof. Suppose that $\gamma \in \Gamma$ is hyperbolic. Then γ has two distinct fixed points on $\mathbb{R} \cup \infty$. Let G be the geodesic in H which joins them. Then, for each point P on G, the point $\gamma(P)$ also lies on G, and some simple integration shows that the distance between P and $\gamma(P)$ is $\log N(\gamma)$ (see [49], Proposition 2.8, for more details). Let us call $G(\gamma, P)$ the (open) geodesic joining P and $\gamma(P)$ in H. This projects down to a closed geodesic $g(\gamma)$ on $\Gamma\backslash H$ of length $\log N(\gamma)$, which does not depend on the choice of P.

Conversely, let g be a closed geodesic on $\Gamma\backslash H$, and let G be a preimage in H. Then G is a geodesic on H and its stabilizer under the action of Γ must contain a hyperbolic element γ (see [48]). For this γ, we have $g = g(\gamma)$.

■

The following Theorem follows immediately from the discussion so far.

Theorem 10 *Let $\Gamma = \Gamma(D, \mathcal{O}, \iota)$ be a cocompact arithemetic Fuchsian group. Let l be the length of a closed geodesic on the quotient surface $\Gamma\backslash H$. Then $\exp(l/2)$ is a Salem number. Conversely, every Salem number is of this form.*

An immediate consequence is that the problem of the existence of a minimal Salem number (cf. Problem 1) is actually equivalent to the following conjecture:

Conjecture 11 (Minimization problem for geodesics) *There is a geodesic of minimal length amongst all closed geodesics on all arithmetic hyperbolic surfaces.*

3.5 Cocompact lattices

In this section we present a simple reformulation of the previous sections in terms of lattices in semi-simple Lie groups.

Theorem 12 (Sury [44], [45]) *The set of Salem numbers is bounded away from 1 if and only if there is a neighborhood of the identity element $U \subset \mathrm{SL}_2(\mathbb{R})$, such that for all cocompact arithmetic Fuchsian groups Γ, the intersection $\Gamma \cap U$ consists only of elements of finite order.*

Proof. We have already seen that the problem of minimizing Salem numbers ϵ is equivalent to the problem of minimizing the traces $\epsilon + 1/\epsilon$ of hyperbolic elements in arithmetic Fuchsian groups. Since hyperbolic matrices have infinite order, the existence of the neighborhood U is equivalent to the statement that the set of these traces is bounded away from 1.

■

T. N. Venkataramana has pointed out to us that a positive answer to (the more general) Problem 2 implies the following conjecture:

Conjecture 13 (Margulis [27]) *Let G be a connected semi-simple group over $\mathbb{R}$. Suppose that $rank_{\mathbb{R}}(G) \geq 2$. Then there is a neighborhood $U \subset G(\mathbb{R})$ of the identity such that for any irreducible cocompact lattice $\Gamma \subset G(\mathbb{R})$, the intersection $\Gamma \cap U$ consists only of elements of finite order.*

We refer the reader to [27] (especially page 322) for the definitions of terms used in this conjecture, and for its connection with Problem 2.

4 Growth rates and pretzel knots

In this section we discuss a restricted class of Salem numbers, that arise both as growth rates for Coxeter groups and as Mahler measures of Alexander polynomials of knots. We solve the minimization problem for this restricted class of Salem numbers (see Theorem 15 and Corollary 20).

4.1 Growth series of Coxeter groups

Let G be any group and S a collection of generators for G. The *growth series for G with respect to S* is the formal power series

$$f(x) = \sum_{n=1}^{\infty} N_S(n) x^n,$$

where $N_S(n)$ is the number of elements in G that can be expressed minimally as a word of length n in the set of generators S. The quantity

$$\lim_{n\to\infty} N_S(n)^{1/n},$$

which is the reciprocal of the radius of convergence of $f(x)$, is called the *asymptotic growth rate* of the group G with respect to the generators S.

We will call a group G a *(planar) Coxeter group* if it is a discrete subgroup of the group of isometries of the spherical, hyperbolic or Euclidean plane generated by a finite set of reflections through geodesic lines (see [14]). The set S of generating reflections is called the set of *standard generators* of the Coxeter group. We will restrict our discussion to those Coxeter groups whose corresponding quotient space is compact.

Steinberg [43] showed that if G is a Coxeter group, and S is a standard set of generators then the corresponding growth series $f(x)$ is a rational function of x (cf. [4]). Floyd and Plotnick ([19], page 503), expanding on Cannon's work [10], show that for any group G of Euclidean, spherical, or hyperbolic planar isometries, the growth series with respect to suitable 'geometric' generators is a reciprocal or anti-reciprocal function:

$$f(x) = \pm f(\frac{1}{x}),$$

up to a factor of $(1-x)$ in some mild exceptional cases. In particular they show that for a Coxeter group (G,S), if $f(x)$ is written as a quotient of relatively prime polynomials, then the denominator $\Delta(x)$ of $f(x)$ is a palindromic polynomial.

Specifically, consider the Coxeter reflection group $G_{p_1,\ldots,p_d}$ generated by reflections through the sides of a spherical, hyperbolic, or planar polygon whose interior angles are

$$\frac{\pi}{p_1}, \ldots, \frac{\pi}{p_d},$$

where $p_1, \ldots, p_d$ are any positive integers. Then (see [14], p. 55) $G_{p_1,\ldots,p_d}$ has the presentation

$$G_{p_1,\ldots,p_d} = \langle\ g_1, \ldots, g_d \mid (g_i)^2 = 1,\ (g_i g_{i+1})^{p_i} = 1\ \rangle.$$

The orbifold Euler characteristic of the quotient surface is given by

$$\chi(G_{p_1,\ldots,p_d}) = \frac{1}{p_1} + \cdots + \frac{1}{p_d} - d + 2.$$

The sign of $\chi(G_{p_1,\ldots,p_d})$ determines whether or not the polygon lives in the hyperbolic, Euclidean, or spherical plane. Accordingly, if $G = G_{p_1,\ldots,p_d}$ and

- if $\chi(G) < 0$, then G is hyperbolic,
- if $\chi(G) = 0$, then G is Euclidean, and,
- if $\chi(G) > 0$, then G is spherical.

Of particular interest to us will be *hyperbolic triangle groups* which are $G_{p,q,r}$, where

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

A picture of the fundamental domain for a (p,q,r)-hyperbolic triangle group is given in Figure 2.

Let $\Delta_{p_1,\ldots,p_d}(x)$ be the denominator of the growth series $f(x)$ of $G_{p_1,\ldots,p_d}$. For any positive integer n, let

$$[n] = 1 + x + \cdots + x^{n-1}.$$

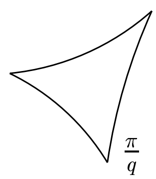

Figure 2. Fundamental domain of a (p, q, r)-hyperbolic triangle group

Theorem 14 (Cannon-Wagreich [10], Floyd-Plotnick [19], Parry [31]) *The polynomial $\Delta_{p_1,\ldots,p_d}(x)$ is given by*

$$\Delta_{p_1,\ldots,p_d}(x) = [p_1]\ldots[p_d](x-d+1) + \sum_{i=1}^{d}[p_1]\ldots\widehat{[p_i]}\ldots[p_d].$$

Furthermore, $\Delta_{p_1,\ldots,p_d}(x)$ is a product of cyclotomic polynomials and at most one Salem polynomial. The Salem polynomial occurs if and only if $G_{p_1,\ldots,p_d}$ is hyperbolic, that is,

$$\frac{1}{p_1} + \cdots + \frac{1}{p_d} < d-2.$$

It follows that the asymptotic growth rate of a hyperbolic Coxeter reflection group with respect to the standard generators is a Salem number.

The polynomials with smallest Mahler measure of degrees 2, 4, 6 and 8 (found by Lehmer in [25]) all arise as factors of $\Delta_{p_1,\ldots,p_d}$ for some positive integers $p_1, \ldots, p_d$ (see [22], Section 3). Also the Lehmer polynomial $L(x) = \Delta_{2,3,7}(x)$ is the denominator of the growth series of the $(2,3,7)$-hyperbolic triangle group.

As the next result shows, the minimization problem has been solved for the family of polynomials $\Delta_{p_1,\ldots,p_d}(x)$.

Theorem 15 (Hironaka [22]) *Lehmer's Salem number ϵ_L is the smallest Salem number arising as a root of $\Delta_{p_1,\ldots,p_d}(x)$, where $p_1, \ldots, p_d$ are any positive integers.*

Essentially, the proof of Theorem 15 (see [22] for more details) comes down to an analysis of the *shape* of the real graphs of $P(x) = \Delta_{p_1,\ldots,p_d}(x)$ when the corresponding Coxeter refection group $G_{p_1,\ldots,p_d}$ is hyperbolic. All of these polynomials, including the Lehmer polynomial shown in Figure 3, have $P(0) = 1$, $P(1) < 0$, and being Salem polynomials, cross the x-axis once in the interval $[0, 1]$, at the point $1/\epsilon$, where ϵ is the corresponding Salem number. One shows that for this particular family the distance of $1/\epsilon$ to 1 is related to the absolute value of the orbifold Euler characteristic, $\chi(G_{p_1,\dots,p_d})$, which is minimized among the hyperbolic planar Coxeter reflection groups, by that of the (2,3,7)-hyperbolic triangle group.

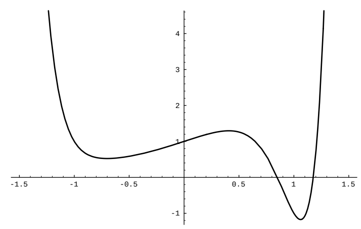

Figure 3. Real graph of the Lehmer polynomial

A suggestive coincidence is that the $(2,3,7)$-hyperbolic triangle also has the smallest volume among hyperbolic polygons. This leads to the question:

Problem 16 *Is there a direct connection between the volumes of hyperbolic polygons and the asymptotic growth rates of the underlying Coxeter reflection groups?*

4.2 Arithmeticity of hyperbolic triangle groups

We will call two discrete groups Γ, $\Gamma' \subset \mathrm{SL}_2(\mathbb{R})$ *commensurable* if $\Gamma \cap \Gamma'$ has finite index in both Γ and Γ'. In this section we will broaden the definition of an arithmetic Fuchsian group given in Section 3.2 to include those Fuchsian groups which, after conjugation in $\mathrm{SL}_2(\mathbb{R})$, are commensurable with groups of the form $\Gamma(D, \mathcal{O}, \iota)$.

Takeuchi shows that there are exactly 85 hyperbolic triangle groups $G_{p,q,r}$ which are arithmetic (although these groups are defined over only 19 totally real fields). Included among these is the triangle group $G_{2,3,7}$.

Recall that the asymptotic growth rate of $G_{2,3,7}$ is equal to ϵ_L, Lehmer's Salem number. Naively, one might hope that, conversely, the arithmetic group associated to ϵ_L is related to $G_{2,3,7}$.

This is, however, not the case. Indeed, in [46], Takeuchi shows that the $(2,3,7)$-hyperbolic triangle group is commensurable to an arithmetic Fuchsian group associated to the totally real field $k_{2,3,7} := \mathbb{Q}(\cos(\frac{\pi}{7}))$. The degree of $k_{2,3,7}$ over $\mathbb{Q}$ is 6, since it is a quadratic extension of the cubic field $\mathbb{Q}(\cos(\frac{2\pi}{7}))$. (This latter field is cubic since it has degree equal to half the degree of the cyclotomic field generated by a primitive 7th root of unity). On the other hand, the totally real field $k_L := \mathbb{Q}(\epsilon_L + 1/\epsilon_L)$ associated to Lehmer's Salem number ϵ_L has degree 5 (half the degree of the Lehmer polynomial).

Comparing degrees shows that ϵ_L is not quadratic over $k_{2,3,7}$, and in particular, ϵ_L can not appear, as described in Section 3.3, as the larger eigenvalue of a hyperbolic matrix in $G_{2,3,7}$. Since ϵ_L *does* appear as the larger eigenvalue of a hyperbolic matrix in $\Gamma = \Gamma(D_\phi, \mathcal{O}, \iota)$, the arithmetic Fuchsian group attached to the division algebra D_ϕ over the totally real field k_L (see Section 3 for an explanation of the notation), we see that $G_{2,3,7}$ and Γ are not isomorphic subgroups of $\mathrm{SL}_2(\mathbb{R})$.

4.3 Alexander polynomials of pretzel links

The Alexander polynomial is a standard integer polynomial invariant of a knot or oriented link L embedded in the three sphere S^3. Since we are interested in Mahler measures, for our purposes it will be useful to define the Alexander polynomial up to a rational multiple, and give a purely algebraic description of the class of Alexander polynomials via Seifert's theorem. For more precise definitions, see, for example, [20] or [33].

Let $M = S^3 \setminus L$ be the complement of L in S^3. The orientations on the components of the link determine an infinite cyclic covering $\widetilde{M}$ of M, and a canonical generator t for the corresponding $\mathbb{Z}$-action on the homology group $\mathcal{H} = H_1(\widetilde{M}; \mathbb{Q})$. The Alexander polynomial is an integer polynomial $P_L(x) \in \mathbb{Z}[x]$, whose roots are the eigenvalues of the action of t on $\mathcal{H}$.

Alexander polynomials form a rich testing ground for the minimization problem, because of the following theorem.

Theorem 17 (Seifert [36]) *$P(x) \in \mathbb{Z}[x]$ is a palindromic polynomial satisfying*

$$P(1) = \pm 1$$

if and only if $P(x)$ is the Alexander polynomial of some knot K.

One is led to ask the following question.

Problem 18 *Can the Mahler measure be minimized for monic, non-cyclotomic Alexander polynomials?*

We restrict our attention to a particular class of knots and links, called *pretzel knots and links*. To describe what they are, we start with the (-2, 3, 7)-pretzel knot. One takes 3 pairs of strings and twists them -2, 3, and 7 times respectively. The negative sign with the 2 means a negative twist. Then one joins the top and bottom strands as in Figure 4.

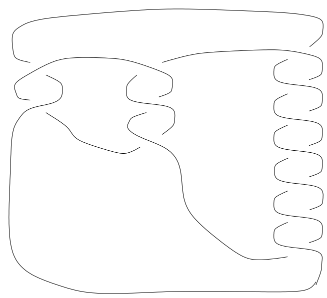

Figure 4. (-2,3,7)-pretzel knot

By replacing (-2, 3, 7) by any list of nonzero integers $(p_1, \ldots, p_d)$, we get a corresponding knot or link $L_{p_1,\ldots,p_d}$, called the $(p_1, \ldots, p_d)$-pretzel knot or link. If $p_1, \ldots, p_d$ are all odd, or at most one is even, then $L_{p_1,\ldots,p_d}$ is a knot, otherwise it is a link with number of components equal to one less than the number of even integers among $p_1, \ldots, p_d$. As described above any choice of orientations on the components of the link determines a one-variable Alexander polynomial for the link. This polynomial may be different for different choices of orientation.

Let $L(x)$ be Lehmer's polynomial. As Kirby points out in his problem list ([24], page 340), $L(-x)$ is the Alexander polynomial of the (-2, 3, 7)-pretzel knot, drawn in Figure 4. This seeming coincidence was also pointed out to the second author by D. Lind.

As mentioned in Section 4.1, Lehmer polynomial $L(x)$ is also the Salem polynomial $\Delta_{2,3,7}(x)$ which is the denominator of the growth series of the (2, 3, 7)-hyperbolic triangle group $G_{2,3,7}$. This leads naturally to the question: is $\Delta_{p_1,\ldots,p_d}(-x)$ also the Alexander polynomial of a pretzel knot or link? This question is answered by the following result.

Theorem 19 (Hironaka [22], Theorem 1.2) *Let d be odd, and let $p_1, \ldots, p_d$ be positive integers. Then the Alexander polynomial of the $(p_1, \ldots, p_d$, -1)- pretzel link, with respect to a suitable orientation of its components, is $\Delta_{p_1,\ldots,p_d}(-x)$.*

This theorem applies to the (-2, 3, 7)-pretzel knot, which is equivalent to the (2, 3, 7, -1)-pretzel knot. The polynomials $\Delta_{p_1,\ldots,p_d}(-x)$ are related to the polynomials arising in Theorem 15. Since $M(P(x)) = M(P(-x))$, for a monic polynomial $P(x) \in \mathbb{Z}[x]$, we have the following corollary.

Corollary 20 *The minimum of the set of Mahler measures of Alexander polynomials of (suitably oriented) $(p_1, \ldots, p_d, \text{-}1)$-pretzel links, as d varies through all odd integers and $p_1, \ldots, p_d$ through all positive integers, is attained by ϵ_L, the Mahler measure of the $(2, 3, 7, \text{-}1)$-pretzel knot.*

So far, questions about Salem numbers and Mahler measures arising from Alexander polynomials of more general links have not been fully addressed. Finding a concrete relation between the geometry of oriented knot and link complements, and the Mahler measures of Alexander polynomials could lead to new insights into Problem 18, and to Lehmer's question itself.

5 Special values of L-functions

We now continue our survey of the ubiquity of Salem numbers in mathematics, by describing how they show up in expressions for the special values of L-functions.

5.1 Stark units and Salem numbers

Given an arbitrary Galois extension K/k of number fields with group G, and a finite-dimensional complex representation $\rho : G \to GL(V)$ one has the Artin L-function

$$L(s, K/k, \rho) = \prod_p \det(1 - Fr_p\big|_{V^{I_p}} Np^{-s})^{-1},$$

where the product runs over all (archimedean) primes p of k, I_p is an inertia subgroup at p, V^{I_p} is the subspace of V of I_p-fixed points, and Fr_p is a Frobenius element at p.

Stark has a conjectural description of the leading term in the Taylor expansion of this L-function at $s = 0$, which states that it is essentially a certain $r \times r$ determinant, where r is the order of vanishing of $L(s, K/k, \rho)$ at $s = 0$. A precise statement can be found in [47]. When $r = 1$, Stark's conjecture is known to be true (see [42]), and the above mentioned determinant is essentially just the logarithm of a special unit of K, now called a *Stark unit.*

We are interested in the case when K/k is a Salem extension, hence of degree 2, and ρ is the non-trivial quadratic character of K/k. In this case we have

$$L(s, K/k, \rho) = \frac{\zeta_K(s)}{\zeta_k(s)},$$

where $\zeta_F(s)$ is the Dedekind zeta function of the number field F. A formula of Dedekind says that the leading term in the Taylor expansion of $\zeta_F(s)$ at $s = 0$

is given by

$$\zeta_F(s) = \frac{h_F R_F}{w_F} s^{s_F+t_F-1} + \text{ higher order terms,}$$

where

- h_F is the class number of F,
- R_F is the regulator of F,
- w_F is the number of roots of 1 in F, and,
- s_F (respectively t_F) is the number of real (respectively complex) places of F.

Using this, we see that when K/k is a Salem extension, $r = 1$, and

$$L'(0, K/k, \rho) = \frac{h_K R_K}{h_k R_k}. \tag{4}$$

The formula (4) is already very close to what is implied by Stark's conjecture. In fact, Stark showed:

Proposition 21 (Stark [42]) *Let K/k be a Salem extension. Then*

$$L'(0, K/k, \rho) = \frac{h_K\, 2^{n-2} \log{(e)}}{h_k\, u} \tag{5}$$

where $u = 2$ when K is generated over k by a square root of a unit of k, and $u = 1$ otherwise, and e is a unit of K, which together with the units of k generates a subgroup of index $2u$ in $\mathcal{O}_K^\times$.

The relation between Stark's conjecture and our subject is seen by the following result.

Proposition 22 (Chinburg [12]) *The unit e of K is a Salem number. Conversely every Salem number ϵ in K is of the form $\epsilon = e^{m/2}$ for some positive integer m.*

Chinburg also uses Proposition 22 to deduce some information on the relative class number h_K/h_k of a Salem extension in [11].

5.2 Lower bounds for relative regulators

The formulas (4) and (5) of the previous section show that one might make some progress towards the minimization problem if one could establish a good absolute lower bound for the quotient of regulators R_K/R_k corresponding to a Salem extension K/k. This observation was made by Costa, Friedman and Skoruppa, who in fact made the following general conjecture which for $r_{L/F} = 1$ implies an affirmative answer to the minimization problem (see [21]):

Conjecture 23 *Let L/F denote an arbitrary extension of number fields, and let*

$$\mathrm{Reg}(L/F) := \frac{1}{[\mathcal{O}_F^\times : \mu_F N_{L/F}(\mathcal{O}_L^\times)]} \frac{R_L}{R_F},$$

where μ_F is the groups of roots of 1 in F. Then there are absolute constants f_0 and f_1 such that:

$$\mathrm{Reg}(L/F) \geq f_0 f_1^{r_{L/F}},$$

where $r_{L/F} \geq 0$ denotes the difference in the unit ranks of L and F.

Costa and Freidman prove Conjecture 23 when $[L : F]$ is 'large', and in the case when L (and so F) is totally real (see [13]).

5.3 Mahler measures and L-values

The results of Section 5.1 point towards a connection between the (logarithms of) Mahler measures of polynomials and the special values of L-functions. In fact the first examples of this phenomena were discovered by Smyth for polynomials in more than one variables. Let $P(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ be such a polynomial. Define its Mahler measure $M(P)$ by

$$\log M(P) = \int \cdots \int_{S^1 \times \cdots \times S^1} |\log P(x_1, \ldots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}.$$

Using Jensen's formula one sees that when $n = 1$ we recover the definition made in the Introduction. In [41] Smyth showed that

$$\log M(1 + x + y) = L'(\chi_{-3}, -1),$$
$$\log M(1 + x + y + z) = 14\, \zeta'(-2),$$

where χ_{-3} is the Dirichlet character attached to the quadratic extension $\mathbb{Q}(\sqrt{-3})$, and $\zeta(s)$ is just the Riemann zeta function. Other striking examples of this kind were given by Ray [32].

The first 'non-abelian' example is due to Deninger [15] and Boyd [9]. They showed

$$\log M(y^2 + (x^2 + x + 1)y + x^2) = L'(E_{15}, 0), \tag{6}$$

where E_{15} is the elliptic curve of conductor 15 defined by the polynomial appearing in (6) above. Actually this formula has only been checked to 50 decimals places of accuracy, though in [15] Deninger has been able to give a heuristic reason for its validity. Moreover in some cases Deninger (see also [3]) has been able to interpret Mahler measures as Deligne periods of mixed motives.

Many other formulae similar to (6) have been numerically identified by Boyd [9], and via different methods, by Rodriguez Villegas [50]. Interestingly, proofs, and not just numerical coincidence, of these formulae have so far been forthcoming mostly for curves E with complex multiplication, in which case both the L-value and the Mahler measure reduce to the value of a Eisenstein-Kronecker series evaluated at the corresponding point of complex multiplication. We refer the reader to the papers mentioned above for more details.

In closing this section we would like to point out a curious discovery of Boyd [9]. Boyd noticed that there is a formula similar to (6) above for $L'(E_{14},0)$ where E_{14} is the elliptic curve over $\mathbb{Q}$ with conductor 14:

$$\log M\big((x+1)y^2+(x^2+x+1)y+(x^2+x)\big) = 0.2274812230.... = L'(E_{14},0).$$

This formula has again only been checked numerically. Since we have (see [8])

$$\lim_{m\to\infty} M(P(x,x^m)) = M(P(x,y)),$$

we see that $\exp(L'(E_{14},0)) = 1.25543...$ is a (potential) limit point of the set of Mahler measures of polynomials in one variable. As it turns out, it is the smallest known limit point.

Now apart from E_{14} there is, up to isogeny, exactly one more elliptic curve over $\mathbb{Q}$ with conductor smaller than 15, namely the curve E_{11} of conductor 11. Yet no such analogous formula has so far been discovered for E_{11}. Since $\exp(L'(E_{11},0)) = 1.16433... < \epsilon_L = 1.17628...$, the existence of such a formula for E_{11} would imply that one would be able to find infinitely many polynomials in one variable, with Mahler measure *smaller* than that of Lehmer's polynomial $L(x)$.

6 Best results and records

This section contains the best results (known to us) concerning lower bounds on Salem numbers and Mahler measures of irreducible monic polynomials $P(x) \in \mathbb{Z}[x]$ in *one* variable.

In 1979, Dobrowolski [16] obtained a lower bound $B(d)$ for the Mahler measure of polynomials of degree d. Since then, his methods have been refined by various mathematicians. As Boyd points out ([8]) the existence of $B(d)$ is not in question since as we have seen (see the proof of Lemma 3) the set of Mahler measures of monic polynomials with integer coefficients of a fixed degree d has a minimal element. In any case, a sample of such a result is the

Theorem 24 (Voutier, [51]) *If $P(X)$ is not a cyclotomic polynomial, and has degree $d > 1$, then*

$$\log M(P) > \frac{1}{4}\Big(\frac{\log(\log(d))}{\log(d)}\Big)^3.$$

Note that the bound above tends to 0 as $d \to \infty$.

One also has bounds that depend on the number of real roots of $P(X)$. For instance it seems that a lower bound for $M(P)$ for those polynomials $P(X)$ which have at least one non-real root outside the unit circle is 1.2013... This is the Mahler measure of the polynomial (cf. [7]):

$$x^{18} + x^{17} + x^{16} - x^{13} - x^{11} - x^9 - x^7 - x^5 + x^2 + x^1 + 1,$$

which has two complex-conjugate roots outside the unit circle. In this vein we have the following theorem (cf. [27], page 322)

Theorem 25 (Laurent) *Let P(X) be a non-cyclotomic polynomial, with r real roots, of degree d. Then*

$$\log M(P) \geq c \, \frac{r^2}{d \log(1 + d/r)},$$

where $c > 0$ is an absolute constant.

Note that for $r = 2$, which is the minimization problem for Salem numbers, this is a better bound than the one above, yet it still tends to 0 as $d \to \infty$.

In closing, we refer the reader to the very informative web page on Lehmer's Conjecture maintained by Mossinghoff [28], where one may find many lists and records related to Problems 1 and 2. For instance, there are tables of the smallest hundred Mahler measures known, the smallest known Mahler measure of each degree $d \leq 180$, the smallest known Mahler measure of a given *height* (= the maximum of the absolute values of the coefficients), the smallest forty-seven Salem numbers less than 1.3 and so on and so forth. There is also a bibliography on Lehmer's conjecture there which nicely compliments our own.

References

[1] E. Artin and J. Tate. *Class Field Theory, Harvard Notes.* W.A. Benjamin, Inc., New York, 1967.

[2] M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, and J.P. Schreiber. *Pisot and Salem numbers.* Birkhauser Verlag, Basel, 1992.

[3] H. Bornhorn. Mahler-masse und speziell werte von L-funktionen. *Preprintreihe, SFB 478 - Geometrische Strukturen in der Mathematik*, ISSN 1435-1188, 1999.

[4] N. Bourbaki. *Groupes et Algèbres de Lie*, volume 13. 1968.

[5] D. W. Boyd. Small salem numbers. *Duke Math. J.*, 44(2):315–328, 1977.

[6] D. W. Boyd. Pisot and salem numbers in intervals of the real line. *Math. Comp.*, 32(144):1244–1260, 1978.

[7] D. W. Boyd. Reciprocal polynomials having small measure. *Math. Comp*, 35(152):1361–1377, 1980.

[8] D. W. Boyd. Speculations concerning the range of Mahler's measure. *Canad. Math. Bull.*, 24(4):453–469, 1981.

[9] D. W. Boyd. Mahler's measure and special values of L-functions. *Experimental Math.*, 7(1):37–82, 1998.

[10] J. W. Cannon and Ph. Wagreich. Growth funcitons of surface groups. *Math. Ann.*, 292:239–257, 1992.

[11] T. Chinburg. On the arithmetic of two constructions of Salem numbers. *J. Reine Angew. Math.*, 348:166–179, 1984.

[12] T. Chinburg. Salem number and L-functions. *J. Number Theory*, 18(2):213–214, 1984.

[13] A. Costa and E. Friedman. Ratios of regulators in totally real extensions of number fields. *J. Number Theory*, 37:288–297, 1991.

[14] H.S.M. Coxeter and W.O.J. Moser. *Generators and Relations for Discrete Groups.* Springer-Verlag, Berlin, 1980.

[15] C. Deninger. K-theory, mixed motives, and the entropy of F^n-actions. *Journal of the A. M. S.*, 10(2):259–281, 1997.

[16] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta. Arith.*, 34(4):391–401, 1979.

[17] G. Everest and T. Ward. *Heights of polynomials and entropy in algebraic dynamics.* Universitext. Springer-Verlag London, Ltd., London, 1999.

[18] V. Flammang, M. Grandcolas, and G. Rhin. Small Salem numbers. In *Number theory in progress*, Zakopane-Kościelisko, 1997, pages 165–168. de Gruyter, Berlin, 1999.

[19] W. J. Floyd and S. P. Plotnick. Symmetries of planar growth functions of Coxeter groups. *Invent. Math.*, 93:501–543, 1988.

[20] R. H. Fox. A quick trip through knot theory. In *Topology of 3-manifolds*, pages 120–167. Prentice-Hall, 1962.

[21] E. Friedman and N-P. Skoruppa. Relative regulators of number fields. *Invent. Math.*, 135:115–144, 1999.

[22] E. Hironaka. The Lehmer polynomial and pretzel knots. *Bull. of Canadian Math. Soc.*, (to appear), 1998.

[23] N. Jacobson. *Basic Algebra II, Second Edition.* W. H. Freeman and Company, New York, 1989.

[24] R. Kirby. Problems in low-dimensional topology. In W. H. Kazez, editor, *Geometric Topology*, Studies in Advanced Mathematics. A.M.S., 1997.

[25] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math.*, 34:461–469, 1933.

[26] D. Lind, K. Schmidt, and T. Ward. Mahler measure and entropy for commuting automorphisms of compact groups. *Invent. Math.*, 101(3):593–629, 1990.

[27] G. A. Margulis. *Discrete subgroups of semisimple Lie groups.* Springer Verlag, 1991.

[28] M. J. Mossinghoff. Lehmer's Conjecture. *http://www.math.ucla.edu/˜mjm.*

[29] M. J. Mossinghoff. Polynomials with small Mahler measure. *Math. Comp.*, 67(3):1697–1705, 1998.

[30] W. D. Neumann and A. W. Reid. Arithmetic of hyperbolic manifolds. In B. Apanasov, W. D. Neumann, A. W. Reid, and L. Siebenmann, editors, *Topology '90*, pages 273–310. Walter de Gruyter and Co., Berlin, 1992.

[31] W. Parry. Growth series of Coxeter groups and Salem numbers. *J. of Alg.*, 154:406–415, 1993.

[32] G. A. Ray. Relations between Mahler's measure and values of L-series. *Can. J. Math.*, 39:694–732, 1987.

[33] D. Rolfsen. *Knots and Links.* Publish or Perish, Inc, Berkeley, 1976.

[34] R. Salem. *Algebraic numbers and Fourier Analysis.* Heath, Boston, MA, 1963.

[35] K. Schmidt. *Dynamical systems of algebraic origin.* Progress in Mathematics, 128. Birkhauser Verlag, Basel, 1995.

[36] H. Seifert. Über das geschlecht von knoten. *Math. Ann.*, 110:571–592, 1934.

[37] J.-P. Serre. Cohomologie des groupes discrets. In *Prospects in Mathematics*, volume 70 of *Ann. Math. Stud.*, pages 77–169. Princeton University Press, 1971.

[38] J.-P. Serre. *Local fields, GTM 67.* Springer-Verlag, Berlin-New York, 1979.

[39] J. Silverman. Small Salem numbers, exceptional units, and Lehmer's conjecture, Symposium on Diophantine Problems (Boulder, CO, 1994). *Rocky Mountain J. Math.*, 26(3):1099–1114, 1996.

[40] C. J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

[41] C. J. Smyth. On measures of polynomials in several variables. *Bull. Austral. Math. Soc.*, 23:49–63, 1981.

[42] H. Stark. L-functions at $s = 1$, II. *Advan. in Math.*, 17:60–92, 1975.

[43] R. Steinberg. Finite reflection groups. *Trans. Amer. Math. Soc.*, 91:493–504, 1959.

[44] B. Sury. Letter to D. Boyd. 1983.

[45] B. Sury. Arithmetic groups and Salem numbers. *Manuscr. Math.*, 75(1):97–102, 1992.

[46] K. Takeuchi. Commensurability classes of arithmetic triangle groups. *Fac. Sci. Univ. Tokyo*, 24(1):201–212, 1977.

[47] J. Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$.* Birkhäuser, 1984.

[48] W. Thurston. *The Geometry and Topology of 3-manifolds.* (unpublished lecture notes), 1977.

[49] M.-F. Vignéras. Arithmetique des algèbres de quaternions. *Springer-Verlag*, LNM 800, 1984.

[50] F. Rodriguez Villegas. Modular Mahler measures I. In S.D. Ahlgren, G. E. Andrews, and K. Ono, editors, *Topics in Number Theory, 1997*, volume 467 of *Mathematics and its Applications.* Kluwer Academic Publishers, Dordrecht, 1999.

[51] P. Voutier. An effective lower bound for the height of algebraic numbers. *Acta. Arith.*, 74(1):81–95, 1996.

Eknath Ghate
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai, 400 005
India
Email: eghate@math.tifr.res.in

Eriko Hironaka
Department of Mathematics
Florida State University
Tallahassee, FL 32306
Email: hironaka@math.fsu.edu