SEVENTY YEARS OF SALEM NUMBERS: A SURVEY

CHRIS SMYTH

Abstract. I survey results about, and recent applications of, Salem numbers.

1. Introduction

In this article I state and prove some basic results about Salem numbers, and then survey some of the literature about them. My intention is to complement other general treatises on these numbers, rather than to repeat their coverage. This applies particularly to the work of Bertin and her coauthors [8, 11, 12] and to the application-rich Salem number survey of Ghate and Hironaka [35]. I have, however, quoted some results from Salem’s classical monograph [80].

Recall that a complex number is an algebraic integer if it is the zero of a polynomial with integer coefficients and leading coefficient 1. Then its (Galois) conjugates are the zeros of its minimal polynomial, which is the lowest degree polynomial of that type that it satisfies. This degree is the degree of the algebraic integer.

A Salem number is an algebraic integer \( \tau > 1 \) of degree at least 4, conjugate to \( \tau^{-1} \), all of whose conjugates, excluding \( \tau \) and \( \tau^{-1} \), lie on \( |z| = 1 \). Then \( \tau + \tau^{-1} \) is a real algebraic integer \( > 2 \), all of whose conjugates \( \neq \tau + \tau^{-1} \) lie in the real interval \( (-2, 2) \). Such numbers are easy to find: an example is \( \tau + \tau^{-1} = 1 + \sqrt{2} \), giving \( (\tau + \tau^{-1} - 1)^2 = 2 \), so that \( \tau^4 - 2\tau^3 + \tau^2 - 2\tau + 1 = 0 \) and \( \tau = 1.8832 \ldots \). We note that this polynomial is a so-called (self)-reciprocal polynomial: it satisfies the equation \( z^{\deg P} P(z^{-1}) = P(z) \). This simply means that its coefficients form a palindromic sequence: they read the same backwards as forwards. This holds for the minimal polynomial of all Salem numbers. It is simply a consequence of \( \tau \) and \( \tau^{-1} \) having the same minimal polynomial. Salem numbers are named after Raphaël Salem, who, in 1945, first defined and studied them [79, Section 6].

2010 Mathematics Subject Classification. Primary 11R06.

Key words and phrases. Salem number.
Salem numbers are usually defined in an apparently more general way, as in the following lemma. It shows that this apparent greater generality is illusory.

**Lemma 1** (Salem [80, p.26]). *Suppose that \( \tau > 1 \) is an algebraic integer, all of whose conjugates \( \neq \tau \) lie in the closed unit disc \( |z| \leq 1 \), with at least one on its boundary \( |z| = 1 \). Then \( \tau \) is a Salem number (as defined above).*

*Proof.* Taking \( \tau' \) to be a conjugate of \( \tau \) on \( |z| = 1 \), we have that \( \bar{\tau}' = \tau' - 1 \) is also a conjugate \( \tau'' \) say, so that \( \tau' = \tau'' \). For any other conjugate \( \tau_1 \) of \( \tau \) we can apply a Galois automorphism mapping \( \tau'' \mapsto \tau_1 \) to deduce that \( \tau_1 = \tau_2^{-1} \) for some conjugate \( \tau_2 \) of \( \tau \). Hence the conjugates of \( \tau \) occur in pairs \( \tau', \tau^{-1} \). Since \( \tau \) itself is the only conjugate in \( |z| > 1 \), it follows that \( \tau^{-1} \) is the only conjugate in \( |z| < 1 \), and so all conjugates of \( \tau \) apart from \( \tau \) and \( \tau^{-1} \) in fact lie on \( |z| = 1 \). \( \square \)

It is known that an algebraic integer lying with all its conjugates on the unit circle must be a root of unity (Kronecker [Kr]). So in some sense Salem numbers are the algebraic integers that are ‘the nearest things to roots of unity’. And, like roots of unity, the set of all Salem numbers is closed under taking powers.

**Lemma 2** (Salem [79, p.169]). *If \( \tau \) is a Salem number of degree \( d \), then so is \( \tau^n \) for all \( n \in \mathbb{N} \).*

*Proof.* If \( \tau \) is conjugate to \( \tau' \) then \( \tau^n \) is conjugate to \( \tau'^n \). So \( \tau^n \) will be a Salem number of degree \( d \) unless some of its conjugates coincide: say \( \tau_1^n = \tau_2^n \) with \( \tau_1 \neq \tau_2 \). But then, by applying a Galois automorphism mapping \( \tau_1 \mapsto \tau \), we would have \( \tau^n = \tau_3^n \) say, where \( \tau_3 \neq \tau \) is a conjugate of \( \tau \), giving \( |\tau^n| > 1 \) while \( |\tau_3^n| \leq 1 \), a contradiction. \( \square \)

Which number fields contain Salem numbers? Of course one can simply choose a list of Salem numbers \( \tau, \tau', \tau'', \ldots \) say, and then the number field \( \mathbb{Q}(\tau, \tau', \tau'', \ldots) \) certainly contains \( \tau, \tau', \tau'', \ldots \). However, if one is interested only in Salem numbers whose degree is that of the field, we can be much more specific.

**Proposition 3** (Salem [79, p.169]). *Suppose that \( K \) is a number field with \( [K : \mathbb{Q}] = d \). Then \( K \) contains a Salem number \( \tau \) of degree \( d \) (equivalently, \( K = \mathbb{Q}(\tau) \) for some Salem number \( \tau \)) if and only if \( K \) has a totally real subfield \( K' \) of index 2, and \( K = K'(\tau) \) with \( \tau + \tau^{-1} = \alpha \), where \( \alpha > 2 \) is an algebraic integer in \( K' \), all of whose conjugates \( \neq \alpha \) lie in \((-2, 2)\).*
If $K = \mathbb{Q}(\tau)$ for some Salem number $\tau$ of degree $d$, then there is a Salem number $\tau_1 \in K$ such that the set of Salem numbers of degree $d$ in $K$ consists of the powers of $\tau_1$.

**Proof.** If $K$ contains a Salem number $\tau$ of degree $d$, then clearly $K = \mathbb{Q}(\tau)$, and so the subfield $K' = \mathbb{Q}(\alpha)$ is totally real, where $\alpha = \tau + \tau^{-1} > 2$, with all its conjugates $\neq \alpha$ lying in $(-2, 2)$. Since $\tau^2 - \alpha \tau + 1 = 0$, we have $[K : K'] = 2$.

Conversely, suppose that $K$ has a totally real subfield $K'$ of index 2, and $K = K'((\alpha))$, where $\alpha > 2$ is an algebraic integer in $K'$, all of whose conjugates $\neq \alpha$ lie in $(-2, 2)$. Then, defining $\tau$ by $\tau^2 - \alpha \tau + 1 = 0$ we have $K = \mathbb{Q}(\tau)$, where $\tau$ is a Salem number.

For the last part, consider the set of all Salem numbers of degree $d$ in $K = \mathbb{Q}(\tau)$. Now the number of Salem numbers $< \tau$ in $K$ is clearly finite, as there are only finitely many possibilities for the minimal polynomials of such numbers. Hence there is a smallest such number, $\tau_1$ say. For any Salem number, $\tau'$ say, in $K$ we can choose a positive integer $r$ such that $\tau_1^r \leq \tau' < \tau_1^{r+1}$. But if $\tau_1^r < \tau'$ then $\tau' \tau_1^{-r}$ would be another Salem number in $K$ which, moreover, would be less than $\tau_1$, a contradiction. Hence $\tau' = \tau_1^r$. \hfill \square

Here we have used the following lemma.

**Lemma 4.** If $\tau' > \tau$ are both Salem numbers of degree $d = [K : \mathbb{Q}]$ in a number field $K$, then $\tau' \tau^{-1}$ is also a Salem number of degree $d$ in $K$.

**Proof.** Since $\tau$ has degree $d$, we have $K = \mathbb{Q}(\tau)$. Hence $\tau'$ is a polynomial in $\tau$. Therefore any Galois automorphism taking $\tau \mapsto \tau^{-1}$ will map $\tau'$ to a real conjugate of $\tau'$, namely $\tau'^{\pm 1}$. But it cannot map $\tau'$ to itself for then, as $\tau$ is also a polynomial in $\tau'$, $\tau$ would be mapped to itself, a contradiction. So $\tau'$ is mapped to $\tau'^{-1}$ by this automorphism. Hence $\tau' \tau^{-1}$ is conjugate to its reciprocal. So the conjugates of $\tau' \tau^{-1}$ occur in pairs $x, x^{-1}$. Again, because $\tau'$ is a polynomial in $\tau$, any automorphism fixing $\tau$ will also fix $\tau'$, and so fix $\tau' \tau^{-1}$. Likewise, any automorphism fixing $\tau'$ will also fix $\tau$.

Next consider any conjugate of $\tau' \tau^{-1}$ in $|z| > 1$. It will be of the form $\tau'_1 \tau_1^{-1}$, where $\tau'_1$ is a conjugate of $\tau'$ and $\tau_1$ is a conjugate of $\tau$. For this to lie in $|z| > 1$, we must either have $|\tau'_1| > 1$ or $|\tau_1| < 1$, i.e., $\tau'_1 = \tau'$ or $\tau_1 = \tau^{-1}$.

But in the first case, as we have seen, $\tau_1 = \tau$, so that $\tau'_1 \tau_1^{-1} = \tau' \tau^{-1}$, while in the second case $\tau'_1 = \tau'^{-1}$, giving $\tau'_1 \tau_1^{-1} = \tau' \tau^{-1} \in |z| < 1$. Hence $\tau' \tau^{-1}$ itself is the only conjugate of $\tau' \tau^{-1}$ in $|z| > 1$. It follows that all conjugates of $\tau' \tau^{-1}$ apart from $(\tau' \tau^{-1})^{\pm 1}$ must lie on $|z| = 1$, making $\tau' \tau^{-1}$ a Salem number.
To show that $\tau'\tau^{-1}$ has degree $d$, consider $d$ automorphisms that map $\tau$ to each of its $d$ conjugates. Then, as we have seen, only the automorphism that maps $\tau$ to itself maps $\tau'\tau^{-1}$ to itself. However, if $\tau'\tau^{-1}$ has degree $d/k$ then there are $k$ such automorphisms mapping $\tau'\tau^{-1}$ to itself. Hence $k = 1$ and $\tau'\tau^{-1}$ has degree $d$. As $\tau$ is a unit, $\tau'\tau^{-1}$ is an algebraic integer, and so is a Salem number.

We now show that the powers of Salem numbers have an unusual property.

**Proposition 5** (Salem [80]). *For every Salem number $\tau$ and every $\varepsilon > 0$ there is a real number $\lambda > 0$ such that the distance $\|\lambda\tau^n\|$ of $\lambda\tau^n$ to the nearest integer is less than $\varepsilon$ for all $n \in \mathbb{N}$. *

**Proof.** We consider the standard embedding of the algebraic integers $\mathbb{Z}(\tau)$ as a lattice in $\mathbb{R}^d$ defined for $k = 0, 1, \ldots, d - 1$ by the map

$$
\tau^k \mapsto (\tau^k, \tau^{-k}, \text{Re} \tau^k_2, \text{Im} \tau^k_2, \text{Re} \tau^k_3, \text{Im} \tau^k_3, \ldots, \text{Re} \tau^{k}_{d/2}, \text{Im} \tau^{k}_{d/2}),
$$

where $\tau^\pm_1, \tau^\pm_j (j = 2, \ldots, d/2)$ are the conjugates of $\tau$. As this is a lattice of full dimension $d$, we know that for every $\varepsilon' > 0$ there are lattice points in the ‘slice’ $\{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_i| < \varepsilon' (i = 2, \ldots, d)\}$. Such a lattice point corresponds to an element $\lambda(\tau)$ of $\mathbb{Z}(\tau)$ with conjugates $\lambda_i$ satisfying $|\lambda_i| < \sqrt{2}\varepsilon' (i = 2, \ldots, d)$.

Next, consider the sums

$$
\sigma_n = \lambda(\tau)\tau^n + \lambda(\tau^{-1})\tau^{-n} + \lambda(\tau_2)\tau^n_2 + \lambda(\tau^{-1}_n)\tau^{-n}_2 + \ldots + \lambda(\tau_{d/2})\tau^n_{d/2} + \lambda(\tau^{-1}_{d/2})\tau^{-n}_{d/2},
$$

where $\lambda(x) \in \mathbb{Z}[x]$. Since $\sigma_n$ is a symmetric function of the conjugates of $\tau$, it is rational. As it is an algebraic integer, it is in fact a rational integer. Since all terms $\lambda(\tau^{-1})\tau^{-n}, \lambda(\tau_2)\tau^n_2, \lambda(\tau^{-1}_n)\tau^{-n}_2, \ldots, \lambda(\tau_{d/2})\tau^n_{d/2}, \lambda(\tau^{-1}_{d/2})\tau^{-n}_{d/2}$ are $< \sqrt{2}\varepsilon'$ in modulus, we see that

$$
|\sigma_n - \lambda(\tau)\tau^n| < (d - 1)\sqrt{2}\varepsilon'.
$$

Hence, choosing $\varepsilon' = \varepsilon/((d - 1)\sqrt{2})$, we have $\|\lambda\tau^n\| \leq |\sigma_n - \lambda(\tau)\tau^n| < \varepsilon$. □

In fact, this property essentially characterises Salem (and Pisot) numbers among all real numbers. Pisot [74] proved that if $\lambda$ and $\tau$ are real numbers such that

$$
\|\lambda\tau^n\| \leq \frac{1}{2\varepsilon \tau(\tau + 1)(1 + \log \lambda)} \quad (1)
$$

for all integers $n \geq 0$ then $\tau$ is either a Salem number or a Pisot number and $\lambda \in \mathbb{Q}(\tau)$.

Recall that a *Pisot number* is an algebraic integer greater than 1 all of whose conjugates, excluding itself, all lie in the open unit disc $|z| <
1. The denominator in this result was later improved by Cantor [24] to $2e\tau(\tau + 1)(2 + \sqrt{\log \lambda})$, and then by Decomps-Guilloux and Grandet-Hugot [26] to $e(\tau + 1)^2(2 + \sqrt{\log \lambda})$. However, Vijayaraghavan [95] proved that for each $\varepsilon > 0$ there are uncountably many real numbers $\alpha > 1$ such that $\|\alpha^n\| < \varepsilon$ for all $n \geq 0$. For a generalisation of this result, and further references in this area, see Bugeaud’s monograph [22, Section 2.4]. To be compatible with (1), it is clear that such $\alpha$ that are not Pisot or Salem numbers must be large (depending on $\varepsilon$). Specifically, if $\alpha > (2e\varepsilon)^{-1/2}$ then there is no contradiction to (1).

For further results concerning the distribution of the fractional parts of $\lambda \tau^n$ for $\tau$ a Salem number, see Dubickas [29] and Zaïmi [96, 97, 98].

2. A smallest Salem number?

Define the polynomial $L(z)$ by

$$L(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1.$$  

This is the minimal polynomial of the Salem number $\tau_{10} = 1.176\ldots$, discovered by D. H. Lehmer [50] in 1933. Curiously, the polynomial $L(-z)$ had appeared a year earlier in Reidemeister’s book [75] as the Alexander polynomial of the $(-2, 3, 7)$ Pretzel knot. Lehmer’s paper seems to be the first where what is now called the Mahler measure of a polynomial appears: the Mahler measure $M(P)$ of a monic one-variable polynomial $P$ is the product $\prod_i \max(1, |\alpha_i|)$ over the roots $\alpha_i$ of the polynomial.

Lehmer also asked whether the Mahler measure of any nonzero noncyclotomic irreducible polynomial with integer coefficients is bounded below by some constant $c > 1$. This is now commonly referred to as ‘Lehmer’s conjecture’ — see [90]. If this were true, then certainly Salem numbers would be bounded away from 1, but this would not immediately imply that there is a smallest Salem number. However, the ‘strong version’ of ‘Lehmer’s conjecture’ states that in fact $c = \tau_{10}$, implying that there is indeed a smallest Salem number, namely $\tau_{10}$. A consequence of this strong version is the following.

**Conjecture 6.** Suppose that $n \in \mathbb{N}$ and $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n$ are real numbers with $\alpha_0 \in (2, \tau_{10} + \tau_{10}^{-1})$ and $\alpha_1, \ldots, \alpha_n \in (-2, 2)$. Then $\prod_{i=0}^{n}(x + \alpha_i) \notin \mathbb{Z}[x]$.

(Note that $\tau_{10} + \tau_{10}^{-1} = 2.026\ldots$) For if there were $\alpha_0, \alpha_1, \ldots, \alpha_n$ in the intervals stated with $\prod_{i=0}^{n}(x + \alpha_i) \in \mathbb{Z}[x]$, then the algebraic integer $\tau > 1$ defined by $\tau + \tau^{-1} = \alpha_0$ would be a Salem number less than $\tau_{10}$.}
3. Construction of Salem numbers

3.1. Salem’s method. Salem [80, Theorem IV, p.30] found a simple way to construct infinite sequences of Salem numbers from Pisot numbers. Now if \( P(z) \) is the minimal polynomial of a Pisot number, then, except possibly for some small values of \( n \), the polynomials \( S_{n,P,\pm 1}(z) = z^n P(z) \pm z^{\deg P} P(z^{-1}) \) factor as the minimal polynomial of a Salem number, possibly multiplied by some cyclotomic polynomials. In particular, for \( P(z) = z^3 - z - 1 \), the minimal polynomial of the smallest Pisot number, \( S_{8,P,1} = (z - 1)L(z) \). Salem’s construction shows that every Pisot number is the limit on both sides of a sequence of Salem numbers. (The construction has to be modified slightly when \( P \) is reciprocal.)

Boyd [14] proved that all Salem numbers could be produced by Salem’s construction, in fact with \( n = 1 \). It turns out that many different Pisot numbers can be used to produce the same Salem number. These Pisot numbers can be much larger than the Salem number they produce. In particular, on taking \( P(z) = z^3 - z - 1 \) and \( \varepsilon = -1 \), the minimal polynomial of the smallest Pisot number \( \theta_0 = 1.3247 \ldots \), Salem’s method shows that there are infinitely many Salem numbers less than \( \theta_0 \). This fact motivates the next definition, due to Boyd.

Salem numbers less than 1.3 are called small. A table of 39 such numbers was compiled by Boyd [14], with later additions of four each by Boyd [16] and Mossinghoff [67], making 47 in all. See the table [68]. (The starred entries in this table are the four Salem numbers found by Mossinghoff. They include one of degree 46.) Further, it was determined by Flammang, Grandcolas and Rhin [33] that the table was complete up to degree 40. This was extended up to degree 44 by Mossinghoff, Rhin and Wu [69] as part of a larger project to find small Mahler measures.

In [17] Boyd showed how to find, for a given \( n \geq 2 \), \( \varepsilon = \pm 1 \) and real interval \([a, b]\), all Salem numbers in that interval that are roots of \( S_{n,P,\varepsilon}(z) = 0 \) for some Pisot number having minimal polynomial \( P(z) \). In particular, of the four new small Salem numbers that he found, two were discovered by this method. The other two he found in [17] are not of this form: they are roots only of some \( S_{1,P,\varepsilon}(z) = 0 \).

Boyd and Bertin [10] investigated the properties of the polynomials \( S_{1,P,\pm 1}(z) \) in detail. For a related, but interestingly different, way of constructing Salem numbers, see Boyd and Parry [21].

Let \( T \) denote the set of all Salem numbers (Salem’s notation). (It couldn’t be called \( S \), because that is used for the set of all Pisot numbers. The
notation $S$ here is in honour of Salem, however: Salem [77] had proved the magnificent result that the Pisot numbers form a closed subset of the real line.) Salem’s construction shows that the derived set (set of limit points) of $T$ contains $S$. Salem [80, p.31] wrote ‘We do not know whether numbers of $T$ have limit points other than $S$’. Boyd [14, p. 327] conjectured that there were no other such limit points, i.e., that the derived set of $S \cup T$ is $S$. (He had recently conjectured [15] that $S \cup T$ is closed – a conjecture that left open the possibility that some numbers in $T$ could be limit points of $T$.)

3.2. **Salem numbers and matrices.** One strategy that has been used to try to prove Lehmer’s Conjecture is to attach some combinatorial object (knot, graph, matrix,. . . ) to an algebraic number (for example, to a Salem number). But it is not clear whether the object could throw light on the (e.g.) Salem number, or, on the contrary, that the Salem number could throw light on the object.

Typically, however, such attachment constructions seem to work only for a restricted class of algebraic numbers, and not in full generality. For example, McKee and Smyth [55] consider integer symmetric matrices as the objects for attachment. (These can be considered as generalisations of graphs: one can identify a graph with its adjacency matrix – an integer symmetric matrix having all entries 0 or 1, with only zeros on the diagonal.) The main tool for their work was the following classical result, which deserves to be better known.

**Theorem 7** (Cauchy’s Interlacing Theorem). *Let $M$ be a real $n \times n$ symmetric matrix, and $M'$ be the matrix obtained from $M$ by removing the $i$th row and column. Then the eigenvalues $\lambda_1, \ldots, \lambda_n$ of $M$ and the eigenvalues $\mu_1, \ldots, \mu_{n-1}$ of $M'$ interlace, i.e.,

$$\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \mu_2 \leq \cdots \leq \mu_{n-1} \leq \lambda_n.$$*

We say that an $n \times n$ integer symmetric matrix $M$ is *cyclotomic* if all its eigenvalues lie in the interval $[-2, 2]$. It is so-called because then its associated reciprocal polynomial

$$P_M(z) = z^n \det \left( (z + z^{-1})I - M \right)$$

has all its roots on $|z| = 1$ and so (Kronecker again) is a product of cyclotomic polynomials. Here $I$ is the $n \times n$ identity matrix.

The cyclotomic graphs are very familiar.
Theorem 8 (J.H. Smith 1969 [87]). The connected cyclotomic graphs consist of the (not necessarily proper) induced subgraphs of the Coxeter graphs \( \tilde{A}_n(n \geq 2), \tilde{D}_n(n \geq 4), \tilde{E}_6, \tilde{E}_7, \tilde{E}_8 \), as in Figure 1.

\[
\begin{align*}
\tilde{A}_n & \quad \tilde{E}_7 & \quad \tilde{E}_8 \\
\tilde{D}_n & \\
\end{align*}
\]

Figure 1. The Coxeter graphs \( \tilde{E}_6, \tilde{E}_7, \tilde{E}_8, \tilde{A}_n(n \geq 2) \) and \( \tilde{D}_n(n \geq 4) \). (The number of vertices is 1 more than the index.)

(These graphs also occur in the theory of Lie algebras, reflection groups, Lie groups, Tits geometries, surface singularities, subgroups of SU\(_2(\mathbb{C})\) (McKay correspondence), . . . .)

McKee and Smyth describe all the cyclotomic matrices, of which the cyclotomic graphs form a small subset. They prove that the strong version of Lehmer’s conjecture is true for the set of polynomials \( P_M \): namely, if \( M \) is not a cyclotomic matrix, then \( P_M \) has Mahler measure at least \( \tau \geq 1 \), the smallest known Salem number. In fact they show that the smallest three known Salem numbers are all Mahler measures of \( P_M \) for some integer symmetric matrix \( M \), while the fourth smallest known Salem number is not.

For other construction methods for Salem numbers see Lakatos [50, 51, 52] and also [59, 55, 56, 57, 58, 88, 89]. In particular, in [50, 52] Lakatos shows that Salem numbers arise as the spectral radius of Coxeter transformations of certain oriented graphs containing no oriented cycles.

3.3. Traces of Salem numbers. McMullen [61, p.230] asked whether there are any Salem numbers of trace less than \(-1\). McKee and Smyth [55, 56] found examples of Salem numbers of trace \(-2\), and indeed showed that there are Salem numbers of every trace. It is known [56] that a Salem number of degree \( d \geq 10 \) has trace at least \( \lfloor 1 - d/9 \rfloor \). In particular, for \( d = 22 \) the trace is at least \(-2\). (For this case this result was obtained earlier by McMullen [37, Cor.1.8], but with the extra restriction that the minimal polynomial \( S(x) \) of the Salem number had \( S(-1) = \pm 1 \) and \( S(1) = \pm 1 \).

3.4. Distribution modulo 1 of the powers of a Salem number. Let \( \tau > 1 \) be a Salem number. Salem [80, Theorem V, p.33] proved that although the powers \( \tau^n \pmod{1} \) of \( \tau \) are everywhere dense on \((0, 1)\), they are
not uniformly distributed on this interval. Further Akiyama and Tanigawa [2] gave a quantitative description of how far this sequence is from being uniformly distributed. They show, for \( \tau \) a Salem number of degree \( 2d' \geq 8 \) and \( \frac{1}{N}A_N(\{\tau^n\}, I) \) being the number of \( n \leq N \) for which the fractional part \( \{\tau^N\} \) lies in a subinterval \( I \) of \([0, 1]\), that \( \lim_{N \to \infty} \frac{1}{N}A_N(\{\tau^n\}, I) \) exists and satisfies

\[
\left| \lim_{N \to \infty} \frac{1}{N}A_N(\{\tau^n\}, I) - |I| \right| \leq 2 \zeta \left( \frac{1}{2} \right) (d' - 1) (2\pi)^{1-d'} |I|.
\]

Here \( |I| \) is the length of \( I \). Note that this difference tends to 0 as \( d' \to \infty \). See also [27].

3.5. **Sumsets of Salem numbers.** Dubickas [28] shows that a sum of \( m \geq 2 \) Salem numbers cannot be a Salem number, but that for every \( m \geq 2 \) there are \( m \) Salem numbers whose sum is a Pisot number and also \( m \) Pisot numbers whose sum is a Salem number.

3.6. **Galois group of Salem number fields.** Lalande [53] and Christopoulos and McKee [25] studied the Galois group of a number field defined by a Salem number. Let \( \tau \) be a Salem number of degree \( 2n \), \( K = \mathbb{Q}(\tau) \) and \( L \) be its Galois closure. Then it is known that \( G := \text{Gal}(L/\mathbb{Q}) \leq C_2^n \rtimes S_n \). Conversely, if \( K \) is a real number field of degree \( 2n > 2 \) with exactly 2 real embeddings, and, for its Galois closure \( L \), that \( G \leq C_2^n \rtimes S_n \), then Lalande proved that \( K \) is generated by a Salem number.

Now, for a Salem number \( \tau \), let \( K' = \mathbb{Q}(\tau + \tau^{-1}) \), \( L' \) be its Galois closure and \( N \subset G \) be the fixing group of \( L' \). Then Christopoulos and McKee showed that \( G \) is isomorphic to \( N \rtimes \text{Gal}(L'/\mathbb{Q}) \), where \( N \) is isomorphic to either \( C_2^n \) or \( C_2^{n-1} \). The latter case is possible only when \( n \) is odd.

Amoroso [3] found a lower bound, conditional on the Generalised Riemann Hypothesis, for the exponent of the class group of such number fields \( L \).

3.7. **The range of polynomials** \( \mathbb{Z}[\tau] \). P. Borwein and Hare [13] studied the ‘spectrum’ of values \( a_0 + a_1 \tau + \cdots + a_n \tau^n \) when the \( a_i \in \{-1, 1\} \), \( n \in \mathbb{N} \) and \( \tau \) is a Salem number. They showed that if \( \tau \) was a Salem number defined by being the zero of a polynomial of the form \( z^m - z^{m-1} - z^{m-2} - \cdots - z^2 - z + 1 \), then this spectrum is discrete. They also asked [13, Section 7]

- Are these the only Salem numbers with this spectrum discrete?
- Are the only \( \tau \) where this spectrum is discrete and \( M(\tau) < 2 \) necessarily Salem numbers or Pisot numbers?
Hare and Mossinghoff [39] show, given a Salem number \( \tau < \frac{1}{2}(1 + \sqrt{5}) \) of degree at most 20, that some sum of distinct powers of \(-\tau\) is zero, so that \(-\tau\) satisfies some Newman polynomial.

Feng [31] remarked that it follows from Garsia [34, Lemma 1.51] that, given a Salem number \( \tau \) and \( m \in \mathbb{N} \) there exists \( c > 0 \) and \( k \in \mathbb{N} \) (depending on \( \tau \) and \( m \)) such that for each \( m \in \mathbb{N} \) there are no nonzero numbers \( \xi = \sum_{i=0}^{n-1} a_i \tau^i \) with \( a_i \in \mathbb{Z}, |a_i| \leq m \) and \( |\xi| < \frac{c}{n^k} \). He asks whether, conversely, if \( \tau \) is any non-Pisot number in \((1, m + 1)\) with this property, then must \( \tau \) necessarily be a Salem number?

### 3.8. Other Salem number studies

Salem [78], [81, p. 35] proved that every Salem number is the quotient of two Pisot numbers.

For connections between small Salem numbers and exceptional units, see Silverman [86].

Dubickas and Smyth [30] studied the lines passing through two conjugates of a Salem number.

Akiyama and Kwon [1] constructed Salem numbers satisfying polynomials whose coefficients are nearly constant.

For generalisations of Salem numbers, see Bertin [6, 7], Cantor [23], Kerada [46], Meyer [66], Samet [81], Schreiber [83] and Smyth [88]. Note the correction made to [81] in [88]. See also Section 4.1 below for 2-Salem numbers.

### 4. Salem numbers outside Number Theory

The survey of Ghate and Hironaka [35] contains many applications of Salem numbers, for the period up to 1999. Only a few of the applications they describe are briefly recalled here, in subsections 4.1, 4.2 and 4.3. Otherwise, I concentrate on developments since their paper appeared.

For some of these applications, the restriction that Salem numbers should have degree at least 4 can be dropped: the results also hold for reciprocal Pisot numbers, whose minimal polynomials are \( x^2 - ax + 1 \) for \( a \in \mathbb{N}, n \geq 3 \). Some authors include these numbers in the definition of Salem numbers. Accordingly, I will allow these numbers to be (honorary!) Salem numbers in this section. Note, however, that for \( \tau \) such a ‘quadratic Salem number’, the fractional parts of the sequence \( \{\tau^n\}_{n\in\mathbb{N}} \) tend to 1 as \( n \to \infty \), whereas for true Salem numbers this sequence is dense in \((0, 1)\), as stated in Section 3.4.

#### 4.1. Growth of groups

For a group \( G \) with finite generating set \( S = S^{-1} \), we define its growth series \( F_{G,S}(x) = \sum_{n=0}^{\infty} a_n x^n \), where \( a_n \) is the number
of elements of $G$ that can be represented as the product of $n$ elements of $S$, but not by fewer. For certain such groups, $F_{G,S}(x)$ is known to be a rational function. Then expanding $F_{G,S}(x)$ out in partial fractions leads to a closed formula for the $a_n$. See [35, Section 4] for a detailed description, including references. See also [4].

In particular, let $G$ be a Coxeter group generated by reflections in $d \geq 3$ geodesics in the upper half plane, forming a polygon with angles $\frac{\pi}{p_i}$ ($i = 1, 2, \ldots, d$), where $\sum_i \frac{\pi}{p_i} < \pi$. Taking $S$ to be the set of these reflections, it is known (Cannon and Wagreich, Floyd and Plotnick, Parry) that then the denominator of $F_{G,S}(x)$ – call it $\Delta_{p_1, p_2, \ldots, p_d}(x)$ – is the minimal polynomial of a Salem number, $\tau$ say, possibly multiplied by some cyclotomic polynomials. Then the $a_n$ grow exponentially with growth rate $\lim_{n \to \infty} a_{n+1}/a_n = \tau$. Hironaka [42] proved that among all such $\Delta_{p_1, p_2, \ldots, p_d}(x)$, the lowest growth rate was achieved for $\Delta_{p_1, p_2, p_3}(x)$, which is Lehmer’s polynomial $L(x)$, with growth rate $\tau_{10} = 1.176\ldots$.

To generalise a bit, define a real 2-Salem number to be an algebraic integer $\alpha > 1$ which has exactly one conjugate $\alpha' \neq \alpha$ outside the closed unit disc, and at least one conjugate on the unit circle. Then all conjugates of $\alpha$ apart from $\alpha \pm 1$ and $\alpha' \pm 1$ have modulus 1. Zerht and Zerht-Liebensdörfer [99] give examples of infinitely many cocompact Coxeter groups ("Coxeter Garlands") in $\mathbb{H}^4$ with the property that their growth function has denominator

$$D_n(z) = p_n(z) + nq_n(z)$$

$$= z^{16} - 2z^{15} + z^{14} - z^{13} + z^{12} - z^{10} + 2z^9 - 2z^8 + 2z^7 - z^6 + z^4 - z^3 + z^2 - 2z + 1$$

$$+ nz(-2z^{14} + z^{12} + z^{10} + z^9 + 2z^7 + z^5 + z^4 + z^2 - 2),$$

which, if irreducible, would be the minimal polynomial of a 2-Salem number.

Umemoto [93] showed that $D_1(t)$ is irreducible$^1$, and also produced infinitely many cocompact Coxeter groups whose growth rate is a 2-Salem number of degree 18. The growth rate in these examples is the larger of the two 2-Salem conjugates that are outside the unit circle. This is compatible with a conjecture of Kellerhals and Perren [45] that the growth rate of a Coxeter group acting on hyperbolic $n$-space should be a Perron number (an algebraic integer $\alpha$ whose conjugates different from $\alpha$ are all of modulus less

---

$^1$In fact, one can show that $D_n(z)$ is irreducible for all $n \geq 1$. A sketch is as follows: comparison with the table [68] shows that neither root of $D_n(z)$ in $|z| > 1$ can be a Salem number. Then putting $z = e^{it}$, the fact that $e^{-3it}p_n(e^{it})/q_n(e^{it})$ is real and $> 0$ for small $t > 0$ shows that $D_n(z)$ has no cyclotomic factors. (Atle Selberg [84, p. 705] remarks that he has always found a sketch of a proof much more informative than a complete proof.)
This has been verified for \( n = 3 \) for so-called generalised simplex groups by Komori and Umemoto [48].

For some other recent papers on non-Salem growth rates see [43], [44], [47].

4.2. Alexander Polynomials. A result of Seifert tells us that a polynomial \( P \in \mathbb{Z}[x] \) is the Alexander polynomial of some knot iff it is monic and reciprocal, and \( P(1) = \pm 1 \). In particular, Hironaka [42] showed that \( \Delta_{p_1, p_2, \ldots, p_d}(-x) \) is the Alexander polynomial of the \((p_1, p_2, \ldots, p_d, -1)\) pretzel knot. Hence, from the result of the previous section, we see that Alexander polynomials are sometimes Salem polynomials (albeit in \(-x\)).

Indeed, Silver and Williams [85], in their study of Mahler measures of Alexander polynomials, found families of links whose Alexander polynomials had Mahler measure equal to a Salem number. The first family \( l(q) \) was obtained [85, Example 5.1] from the link \( 7_1^2 \) by giving \( q \) full right-handed twists to one of the components as it passed through the other component (the trivial knot). The Mahler measure of the Alexander polynomials of these links produced a decreasing sequence of Salem numbers for \( q = 1, 2, \ldots, 11 \). For \( q = 10 \) the Salem number \( 1.18836 \ldots \) (the second-smallest known) was produced, with minimal polynomial

\[
x^{18} - x^{17} + x^{16} - x^{15} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 - x^3 + x^2 - x + 1,
\]

while \( q = 11 \) gave the Salem number \( M(L(x)) = 1.17628 \ldots \). For \( q > 11 \) Salem numbers were not produced. The second example was obtained in a similar way [85, Example 5.8], using the link formed from the knot \( 5_1^1 \) by adding the trivial knot encircling two strands of the knot, and then giving these strands \( q \) full right-hand twists. For increasing \( q \geq 3 \) this gave a monotonically increasing sequence of Salem numbers tending to the smallest Pisot number \( \theta_0 = 1.3247 \ldots \). These Salem numbers are equal to

\[
M(x^{2(q+1)}(x^3-x-1)+x^3+x^2-1). 
\]

Furthermore, \( M(x^n(x^3-x-1)+x^3+x^2-1) \) is also a Salem number for \( n \geq 9 \) and odd. Silver (private communication) has shown that these Salem numbers are also Mahler measures of Alexander polynomials: “Putting an odd number of half-twists in the rightmost arm of the pretzel knot produces 2-component links rather than knots. Their Alexander polynomials have two variables. However, setting the two variables equal to each other produces the so-called 1-variable Alexander polynomials, and indeed the ‘odd’ sequence of Salem polynomials . . . results.”

4.3. Lengths of closed geodesics. It is known that there is a bijection between the set of Salem numbers and the set of closed geodesics on certain
arithmetic hyperbolic surfaces. Specifically, the length of the geodesic is \(2 \log \tau\), where \(\tau\) is the Salem number corresponding to the geodesic. Thus there is a smallest Salem number iff there is a geodesic of minimal length among all closed geodesics on all arithmetic hyperbolic surfaces. See Ghate and Hironaka [35, Section 3.4] and also Maclachlan and Reid [60, Section 12.3] for details.

4.4. **Arithmetic Fuchsian groups.** Neumann and Reid [70, Lemmas 4.9, 4.10] have shown that Salem numbers are precisely the spectral radii of hyperbolic elements of arithmetic Fuchsian groups. See also [35], [60, pp. 378–380] and [54, Theorem 9.7].

The following result is related.

**Theorem 9 (Sury [92]).** The set of Salem numbers is bounded away from 1 iff there is some neighbourhood \(U\) of the identity in \(\text{SL}_2(\mathbb{R})\) such that, for each arithmetic cocompact Fuchsian group \(\Gamma\), the set \(\Gamma \cap U\) consists only of elements of finite order. (A Fuchsian group is a group \(\Gamma\) discrete in \(\text{SL}_2(\mathbb{R})\) and such that \(\Gamma \backslash \mathbb{H}\) has finite volume.)

4.5. **A dynamical system.** For given \(\beta > 1\), define the map \(T_\beta : [0, 1] \to [0, 1]\) by \(T_\beta x = \{\beta x\}\), the fractional part of \(\beta x\). Then from \(x = \frac{\lfloor \beta x \rfloor}{\beta} + \frac{T_\beta x}{\beta}\)

we obtain the identity \(x = \sum_{n=1}^{\infty} \frac{\lfloor \beta T_\beta^{n-1} x \rfloor}{\beta^n}\), the (greedy) \(\beta\)-expansion of \(x\) [73].

Klaus Schmidt [82] showed that if the orbit of 1 is eventually periodic for all \(x \in \mathbb{Q} \cap [0, 1]\) then \(\beta\) is a Salem or Pisot number. He also conjectured that, conversely, for \(\beta\) a Salem number, the orbit of 1 is eventually periodic. This conjecture was proved by Boyd [18] to hold for Salem numbers of degree 4. However, using a heuristic model in [20], his results indicated that while Schmidt’s conjecture was likely to also hold for Salem numbers of degree 6, it may be false for a positive proportion of Salem numbers of degree 8. Recently, computational degree-8 evidence supporting Boyd’s model was compiled by Hichri [41]. As Boyd points out, the basic reason seems to be that, for \(\beta\) a Salem number of degree \(d\), this orbit corresponds to a pseudorandom walk on a \(d\)-dimensional lattice. Under this model, but assuming true randomness, the probability of the walk intersecting itself is 1 for \(d \leq 6\), but is less than 1 for \(d > 6\).

Hare and Tweddle [40, Theorem 8] give examples of Pisot numbers for which the sequences of Salem numbers from Salem’s construction that tend to the Pisot number from above have eventually periodic orbits. See also [19].
4.6. **Surface automorphisms.** A *K3 surface* is a simply-connected compact complex surface $X$ with trivial canonical bundle. The intersection form on $H^2(X, \mathbb{Z})$ makes it into an even unimodular 22-dimensional lattice of signature $(3,19)$; see [65, p.17]. Now let $F : X \to X$ be an automorphism of positive entropy of a K3 surface $X$. Then McMullen [61, Theorem 3.2] has proved that the spectral radius $\lambda(F)$ (modulus of the largest eigenvalue) of $F$ acting by pullback on this lattice is a Salem number. More specifically, the characteristic polynomial $\chi(F)$ of the induced map $F^*|H^2(X, \mathbb{R}) \to H^2(X, \mathbb{R})$ is the minimal polynomial of a Salem number multiplied by $k \geq 0$ cyclotomic polynomials. Since $\chi(F)$ has degree 22, the degree of $\lambda(F)$ is at most 22. (If $X$ is projective, $X$ has Picard group of rank at most 20, and so $\lambda(F)$ has degree at most 20.)

It is an interesting problem to describe which Salem numbers arise in this way. McMullen [61] found 10 Salem numbers of degree 22 and trace $-1$, also having some other properties, from which he was able to construct from each of these Salem numbers a K3 surface automorphism having a Siegel disc. (These were the first known examples having Siegel discs). Gross and McMullen [37] have shown that if the minimal polynomial $S(x)$ of a Salem number of degree 22 has $|S(-1)| = |S(1)| = 1$ (which they call the unramified case) then it is the characteristic polynomial an automorphism of some (non-projective) K3 surface $X$. (If the entropy of $F$ is 0 then this characteristic polynomial is simply a product of cyclotomic polynomials.)

It is known (see [61, p.211] and references given there) that the topological entropy $h(F)$ of $F$ is equal to $\log \lambda(F)$, so is either 0 or the logarithm of a Salem number.

For each even $d \geq 2$ let $\tau_d$ be the smallest Salem number of degree $d$. McMullen [63, Theorem 1.2] has proved that if $F : X \to X$ is an automorphism of any compact complex surface $X$ with positive entropy, then $h(F) \geq \log \tau_{10} = \log(1.176 \ldots) = 0.162 \ldots$. Bedford and Kim [5] have shown that this lower bound is realised by a particular rational surface automorphism. McMullen [64] showed that it was realised for a non-projective K3 surface automorphism, and later [65] that it was realised for a projective K3 surface automorphism. He showed that the value $\log \tau_d$ was realised for a projective K3 surface automorphism for $d = 2, 4, 6, 8, 10$ or 18, but not for $d = 14, 16, \text{or} 20$. (The case $d = 12$ is currently undecided.)

Oguiso [72] remarked that, as for K3 surfaces (see above), the characteristic polynomial of an automorphism of arbitrary compact Kähler surface is
also the minimal polynomial of a Salem number multiplied by \( k \geq 0 \) cyclotomic polynomials. This is because McMullen’s proof for K3 surfaces in [61] is readily generalised. In another paper [71] he proved that this result also held for automorphisms of hyper-Kähler manifolds. Oguiso [72] also constructed an automorphism \( F \) of a (projective) K3 surface with \( \lambda(F) = \tau_{14} \). Here the K3 surface was projective, contained an \( E_8 \) configuration of rational curves, and the automorphism also had a Siegel disc.

Reschke [76] studied the automorphisms of two-dimensional complex tori. He showed that the entropy of such an automorphism, if positive, must be a Salem number of degree at most 6, and gave necessary and sufficient conditions for such a Salem number to arise in this way.

4.7. Salem numbers and Coxeter systems. Consider a Coxeter system \((W, S)\), consisting of a multiplicative group \( W \) generated by a finite set \( S = \{s_1, \ldots, s_n\} \), with relations \((s_is_j)^{m_{ij}} = 1\) for each \( i, j \), where \( m_{ii} = 1 \) and \( m_{ij} \geq 2 \) for \( i \neq j \). The \( s_i \) act as reflections on \( \mathbb{R}^n \). For any \( w \in W \) let \( \lambda(w) \) denote its spectral radius. This is the modulus of the largest eigenvalue of its action on \( \mathbb{R}^n \). Then McMullen [62, Theorem 1.1] shows that when \( \lambda(w) > 1 \) then \( \lambda(w) \geq \tau_{10} = 1.176 \ldots \). This could be interpreted as circumstantial evidence for \( \tau_{10} \) indeed being the smallest Salem number.

The Coxeter diagram of \((W, S)\) is the weighted graph whose vertices are the set \( S \), and whose edges of weight \( m_{ij} \) join \( s_i \) to \( s_j \) when \( m_{ij} \geq 3 \). Denoting by \( Y_{a,b,c} \) the Coxeter system whose diagram is a tree with 3 branches of lengths \( a, b \) and \( c \), joined at a single node, McMullen also showed that the smallest Salem numbers of degrees 6, 8 and 10 coincide with \( \lambda(w) \) for the Coxeter elements of \( Y_{2,3,7}, Y_{2,4,5} \) and \( Y_{3,3,4} \) respectively. In particular, \( \lambda(w) = \tau_{10} \) for the Coxeter elements of \( Y_{2,3,7} \).

4.8. Dilatation of pseudo-Anosov automorphisms. For a closed connected oriented surface \( S \) having a pseudo-Anosov automorphism that is a product of two positive multi-twists, Leininger [54, Theorem 6.2] showed that its dilatation is at least \( \tau_{10} \). This follows from McMullen’s work on Coxeter systems quoted above. The case of equality is explicitly described (in particular, \( S \) has genus 5). (However, on surfaces of genus \( g \) there are examples of pseudo-Anosov automorphisms having dilatations equal to \( 1 + O(1/g) \) as \( g \to \infty \). These are not Salem numbers when \( g \) is sufficiently large.)

4.9. Bernoulli convolutions. Following Solomyak [91], let \( \lambda \in (0, 1) \), and \( Y_\lambda = \sum_{n=0}^{\infty} \pm \lambda^n \), with the \( \pm \) chosen independently ‘+’ or ‘–’ each with probability \( \frac{1}{2} \). Let \( \nu_\lambda(E) \) be the probability that \( Y_\lambda \in E \), for any Borel set.
E. So it is the infinite convolution product of the means \( \frac{1}{2}(\delta - \lambda^n + \delta \lambda^n) \) for \( n = 0, 1, 2, \ldots, \infty \), and so is called a Bernoulli convolution. Then \( \nu_\lambda(E) \) satisfies the self-similarity property

\[
\nu_\lambda(E) = \frac{1}{2} \left( \nu_\lambda(S_1^{-1}E) + \nu_\lambda(S_2^{-1}E) \right),
\]

where \( S_1 x = 1 + \lambda x \) and \( S_2 x = 1 - \lambda x \). It is known that the support of \( \nu_\lambda \) is a Cantor set of zero length when \( \lambda \in (0, \frac{1}{2}) \), and the interval \([-\lambda^{-1} - 1, \lambda^{-1} - 1] \) when \( \lambda \in (\frac{1}{2}, 1) \). When \( \lambda = \frac{1}{2} \), \( \nu_\lambda \) is the uniform measure on \([-2, 2]\). Now the Fourier transform \( \hat{\nu}_\lambda(\xi) \) of \( \nu_\lambda \) is equal to \( \prod_{n=0}^{\infty} \cos(\lambda^n \xi) \). Salem [81, p. 40] proved that if \( \lambda \in (0, 1) \) and \( 1/\lambda \) is not a Pisot number, then \( \lim_{\xi \to \infty} \hat{\nu}_\lambda(\xi) = 0 \). This contrasts with an earlier result of Erdős that if \( \lambda = \frac{1}{2} \) and \( 1/\lambda \) is a Pisot number, then \( \hat{\nu}_\lambda(\xi) \) does not tend to 0 as \( \xi \to \infty \). Recently Feng [31] has studied \( \nu_\lambda \) when \( 1/\lambda \) is a Salem number, proving in this case that \( \nu_\lambda \) the corresponding measure \( \nu_\lambda \) is a multifractal measure satisfying the multifractal formalism in all of the increasing part of its multifractal spectrum.

**Acknowledgements.** This paper is an expanded version of a talk that I gave at the meeting ‘Growth and Mahler measures in geometry and topology’ at the Mittag-Leffler Institute, Djursholm, Sweden, in July 2013. I would like to thank the organisers Eriko Hironaka and Ruth Kellerhals for the invitation to attend the meeting, and to thank them, the Institute staff and fellow participants for making it such a stimulating and pleasant week.

I also thank David Boyd, Yann Bugeaud, Eriko Hironaka, Aleksander Kolpakov, James McKee, Curtis McMullen, Dan Silver and Joe Silverman for their very helpful comments and corrections on earlier drafts of this survey.

I would be pleased to hear from readers of any remaining errors or omissions.

**References**


[41] Lakatos, Piroska, Salem numbers defined by Coxeter transformation. Linear Algebra Appl. 432 (2010), no. 1, 144-154.


[68] List of small Salem numbers.
http://www.cecm.sfu.ca/~mjm/Lehmer/lists/SalemList.html


School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, Edinburgh, EH9 3JZ, Scotland
E-mail address: c.smyth@ed.ac.uk