1. Characterization of some interesting subsets of Salem numbers—Bertin-Boyd’s results

Consider the construction

\[ Q(z) = zP(z) + \epsilon P^*(z) \]

Boyd and myself [BB95] observed that they are two particular classes of polynomial \( P \) for which we can be sure that \( Q(z) \) has at most one zero in \( |z| > 1 \).

**A:** \( P \) has no zero in \( |z| \leq 1 \). Then \( zP(z) \) has one zero in \( |z| < 1 \) and \( n \) zeros in \( |z| > 1 \). The branches starting at the \( n \) zeros in \( |z| > 1 \) end at points in \( |z| \geq 1 \) so \( Q \) has at least \( n \) zeros in \( |z| \geq 1 \) and hence at most one zero in \( |z| < 1 \) (the end of the branch starting at 0). Since \( Q \) is reciprocal, it thus has at most one zero in \( |z| > 1 \). If there is such a zero it must be \( \pm \tau \) for a Salem number \( \tau \) (or reciprocal quadratic). This was the choice considered in Bertin’s thesis [Be81].

**B:** \( P \) has a single zero in \( |z| > 1 \) so \( zP(z) \) has \( n \) zeros in \( |z| < 1 \). The above argument can be repeated by considering the fate of the \( n \) branches beginning at these zeros. This was the case considered by Salem [Sa45] and Boyd [Bo78]. In this case, if the zero \( \theta \) of \( P(z) \) in \( |z| > 1 \) satisfies \( \theta > 1 \), then \( \theta \) is a Pisot number and \( P(z) = z^{m-1}P_0(z) \) where \( P_0 \) is the minimal polynomial of \( \theta \). If \( Q \) has a zero in \( |z| > 1 \) then it is a Salem number (or reciprocal quadratic).

Note that if \( Q \) has one zero in \( |z| > 1 \) and hence \( n - 1 \) zeros on \( |z| = 1 \) then these are all entrances in case (A) and exits in case (B).

Given any \( Q \) with integer coefficients reciprocal or antireciprocal, with a single root in \( |z| > 1 \) and simple roots on \( |z| = 1 \), and given \( k \) with \( 1 \leq k \leq n \), it was shown in the previous section that they are monic polynomials \( P \) with integer coefficients satisfying (1) with exactly \( k \) zeros in \( |z| > 1 \) and \( n - k \) zeros in \( |z| < 1 \). **Thus any such class of \( P \), in particular (A) or (B), can be used to generate all Salem numbers.**

The classes (A) and (B) have the advantage that they generate only Salem numbers, reciprocal quadratics, and roots of unity. Note, in these two cases, that the restriction that \( Q \) have simple roots on \( |z| = 1 \) is necessary since an multiple root must be both an exit and an entrance.

**Definition 1.** The set \( A_q \) is the set of Salem numbers produced by (A) with \( |P(0)| = q \) and \( \epsilon = -sgnP(0) \).
The set $B_q$ is the set of Salem numbers produced by (B) with $|P(0)| = q$ and $\epsilon = sgn P_0(0)$ where $P(z) = z^{m-1} P_0(z)$, $P_0(0) \neq 0$.

Remark 2. The set $A_q = \mathcal{T}_q \cap T$ where $\mathcal{T}_q$ was the set introduced by Bertin in [Be81] and $T$ the set of Salem numbers. In particular it was shown there that $A_q$ is bounded above by $q + (q^2 - 1)^{1/2}$. Note that if $\epsilon = 1$ then the restriction $P(0) = -q$ is needed to insure that $Q(1) < 0$ so that $Q$ has a zero $\tau > 1$. Moreover since all zeros of $P$ are in $|z| > 1$ we must have $q \geq 2$ in case (A).

Remark 3. The sets $B_q$ were considered by Boyd in [Bo78]. When $q = 0$, $P(z) = z^{m-1} P_0(z)$ with $m > 1$ so $B_q = \{ \theta_m, m > 1 \}$ in the notation [Bo77], [Bo78] while $B_q = \{ \theta_1; |N(\theta)| = q, \epsilon = sgn N(\theta) \}$.

Remark 4. By the result of [Bo80] mentionned above,

$$T = \bigcup_q A_q = \bigcup_q B_q.$$ 

Given $c > 1$, the hope was the existence of $M$ such that $T \cap [1, c]$ be contained in the finite union $\bigcup_{2 \leq q \leq M} A_q$ or $\bigcup_{0 \leq q \leq M-2} B_q$.

Remark 5. The set $B_0 \cap \{9/8, 13/10\}$ was enumerated in [Bo78].

1.0.1. Examples of small Salem numbers in $A_2$. In 1980, I tempted to determine the smallest Salem numbers of the set $A_2$. Using an adapted version of the Schur's algorithm, I found for example.

$\sigma_1$ is zero of three different polynomials

$$z = \frac{1 + 2z + z^2 - z^3 - z^4 - z^5 - z^6 - z^7 + 2z^9 + 2z^{10}}{2 + 2z - z^3 - z^4 - z^5 - z^6 - z^7 + z^8 + 2z^9 + z^{10}}$$

$$z = \frac{1 + 2z + z^2 + z^8 + 2z^9 + 2z^{10}}{2 + 2z + z^2 + z^6 + 2z^8 + z^{10}}$$

$$z = \frac{1 + 2z + 2z^2 + 2z^3 + 3z^4 + 4z^5 + 4z^6 + 3z^7 + 3z^8 + 3z^9 + 2z^{10}}{2 + 3z + 3z^2 + 3z^3 + 4z^4 + 4z^5 + 3z^6 + 2z^7 + 2z^8 + 2z^9 + z^{10}}$$

$\sigma_2$ is zero of the polynomial

$$z = \frac{1 + 2z^2 + z^4 - z^6 - 2z^8 - 2z^{10} - 2z^{12} + 2z^{16} + 2z^{18}}{2 + 2z^2 - 2z^6 - 2z^8 - z^{10} - z^{12} + z^{14} + 2z^{16} + z^{18}}$$

$\sigma_3$ is zero of the polynomial

$$z = \frac{1 + 2z^2 + z^4 - z^6 - 2z^8 - 2z^{10} + 2z^{14} + 2z^{16}}{2 + 2z^2 - 2z^6 - 2z^8 - z^{10} + z^{12} + 2z^{14} + z^{16}}$$

$\sigma_5$ is zero of five polynomials

$$z = \frac{1 + z + z^2 + 2z^3 + 2z^4 + 2z^5 + 2z^6 + 3z^7 + 2z^8 + z^9 + 2z^{10}}{2 + z + 2z^2 + 3z^3 + 2z^4 + 2z^5 + 2z^6 + 2z^7 + z^8 + z^9 + z^{10}}$$

$$z = \frac{1 + 2z^2 + z^4 - z^6 - 2z^8 + 2z^{12} + 2z^{14}}{2 + 2z^2 - 2z^6 - z^8 + z^{10} + 2z^{12} + z^{14}}$$

$$z = \frac{1 + z + 2z^2 + 2z^3 + z^4 + z^5 + z^6 + 2z^7 + 2z^8 + 2z^9 + 2z^{10}}{2 + 2z + 2z^2 + 2z^3 + z^4 + z^5 + z^6 + 2z^7 + 2z^8 + z^9 + z^{10}}$$

$$z = \frac{1 + z + z^3 - z^4 - z^6 - z^7 - 2z^9 - z^{11} + z^{13} + 2z^{15}}{2 + z^2 - z^4 - 2z^6 - z^8 - z^9 - z^{11} + z^{12} + z^{14} + z^{15}}$$

1
\[ z = \frac{1 + z + z^3 - z^4 - z^5 - z^6 + z^8 + 2z^{10}}{2 + z^2 - z^4 - z^5 - z^6 + z^7 + z^9 + z^{10}} \]

\( \sigma_6 \) is root of the polynomial
\[ z = \frac{1 + z^2 - z^8 - 2z^{10} + 2z^{18}}{2 - 2z^8 - z^{10} + z^{16} + z^{18}} \]

\( \sigma_{10} \) is root of the polynomial
\[ z = \frac{1 + z^2 - z^8 + 2z^{16}}{2 - z^8 + z^{14} + z^{16}} \]

\( \sigma_{16} \) is root of the polynomial
\[ z = \frac{1 + z^2 - z^4 - z^6 + z^{10} - 2z^{14} + 2z^{18}}{2 - 2z^4 + z^8 - z^{12} - z^{14} + z^{16} + z^{18}} \]

1.0.2. Characterization of the sets \( A_q \) and \( B_q \).

**Theorem 6** (Theorem A). Suppose that \( \tau \) is a Salem number with minimal polynomial \( T \). Then \( \tau \) is in \( A_q \) if and only if there is a cyclotomic polynomial \( K \) with simple roots and \( K(1) \neq 0 \) and a reciprocal polynomial \( L \) with the following properties:

1. \( L(0) = q - 1 \)
2. \( \deg L = \deg(KT) - 1 \)
3. \( L(1) \geq -K(1)T(1) \)
4. \( L \) has all its zeros on \( |z| = 1 \) and they interlace the zeros of \( KT \) on \( |z| = 1 \) in the following sense: let \( e^{i\psi_1}, ..., e^{i\psi_m} \) be the zeros of \( L \) with \( \Im z \geq 0 \), excluding \( z = -1 \), with \( 0 < \psi_1 < ... < \psi_m < \pi \), and let \( e^{i\phi_1}, ..., e^{i\phi_m} \) be the zeros of \( KT \) on \( |z| = 1 \), \( \Im z \geq 0 \), with \( 0 < \phi_1 < ... < \phi_m \leq \pi \); then
\[
0 < \psi_1 < \phi_1 < ... < \psi_m < \phi_m.
\]

**Theorem 7** (Theorem B). Suppose that \( \tau \) is a Salem number with minimal polynomial \( T \). Then \( \tau \) is in \( B_q \) if and only if there is a cyclotomic polynomial \( K \) with simple roots and \( K(1) \neq 0 \) and a reciprocal polynomial \( L \) with the following properties:

1. \( L(0) = q + 1 \)
2. \( \deg L = \deg(KT) - 1 \)
3. \( L(1) \geq K(1)T(1) \)
4. \( L \) has all its zeros on \( |z| = 1 \) and they interlace the zeros of \( KT \) on \( |z| = 1 \) in the following sense: let \( e^{i\psi_1}, ..., e^{i\psi_m} \) be the zeros of \( L \) with \( \Im z \geq 0 \), excluding \( z = -1 \), with \( 0 < \psi_1 < ... < \psi_m < \pi \), and let \( e^{i\phi_1}, ..., e^{i\phi_m} \) be the zeros of \( KT \) on \( |z| = 1 \), \( \Im z \geq 0 \), with \( 0 < \phi_1 < ... < \phi_m \leq \pi \); then
\[
0 < \phi_1 < \psi_1 < ... < \psi_m < \phi_m.
\]

**Remark 8.** For proofs of Theorem (A) and Theorem (B) we refer to [BB95].

In case \( Q = zP - P^* \), we can write \( (z - 1)Q_1 = zZ - P^* \) and we can take \( L = P - Q_1 \).

**Corollary 9.**
\[ A_q \subset B_{q-2} \text{ for } q \geq 2. \]

**PROOF.** The conditions of Theorem (B) are weaker than the corresponding conditions of Theorem (A). \qed
Corollary 10. \( A_q \subset A_{kq-k+1} \) for \( q \geq 2, k \geq 1 \)

**PROOF.** If \( L \) satisfies Theorem (A) with \( L(0) = q - 1 \), then \( kL \) satisfies the theorem with \( kL(0) = kq - k \) showing \( \tau \) is in \( A_{kq-k+1} \). \( \square \)

**Theorem 11.** Denote \( C \) the list of 43 smallest known Salem numbers called \( \sigma_1, \ldots \) of Mossinghoff's list except \( \ast \sigma_{39}, \ast \sigma_{40}, \ast \sigma_{43}, \ast \sigma_{46} \) discovered later.

We have the inclusion

\[ A_2 \subset C \setminus \{ \sigma_{20}, \sigma_{23}, \sigma_{28}, \sigma_{31}, \sigma_{33}, \sigma_{35} \} \]

**PROOF.** To show that \( \sigma_k \) belongs to \( A_2 \) it generally suffices to take \( K = 1 \) and to produce by inspection a suitable cyclotomic polynomial \( L \) whose zeros interlace those of \( KT \).

To show that a given \( \sigma_k \) is not in \( A_2 \), one can rely on the algorithm of [Bo78] which enumerates all the possible representations of \( \sigma_k \) as an element of \( B_0 \). For example, \( \sigma_{33} \), which is of degree 34, has just one such representation and this shows that the only choices of \( K \) and \( L \) are \( K = 1 \) and \( L = (z^4 - 1)(z^{29} - 1) \). Since \( L(1) = 0 \), this does not satisfy Theorem (A), so \( \sigma_{33} \notin A_2 \). \( \square \)

2. A MINORATION OF SALEM NUMBERS

Most of known minorations of \( \tau \), if \( \tau \) is a Salem number depend on the degree of the Salem polynomial (Dobrowolski, Voutier, etc use transcendental methods). Another, though not the sharpest is the elegant minoration due to Smyth (1980)

\[ \tau > 1 + \frac{c}{d} \]

c being a constant and \( d \) denoting the degree of the Salem number.

We have seen in the previous section that the conjugates of modulus 1 of the smallest known Salem numbers offer a certain regularity, interlacing property with roots of unity. We propose here a minoration using the discriminant of the Salem polynomial or its trace polynomial [Be95]. And again we shall see a certain regularity of the discriminants.

**Definition 12.** Let \( T \) a Salem polynomial of degree \( 2s \). We call trace polynomial of \( T \), the monic polynomial \( Q \), \( Q \in \mathbb{Z}[X] \), of degree \( s \), satisfying

\[ X^sQ(X + \frac{1}{X}) = T(X). \]

For example, if \( T \) is the Salem polynomial of degree 6 of the Salem number \( \tau = 1.401288 \ldots \),

\[ T(X) = X^6 - X^4 - X^3 - X^2 + 1, \]

its trace polynomial is

\[ Q(Y) = Y^3 - 4Y - 1. \]

Denoting by \( \tau, \frac{1}{\tau}, \tau(j), \frac{1}{\tau(j)}, 2 \leq j \leq s \), the roots of \( T \), then the roots of the trace polynomial are \( \tau + \frac{1}{\tau}, \tau(j) + \frac{1}{\tau(j)} \) thus all real between \(-2, 2 \) except \( \tau + \frac{1}{\tau} > 2 \).

If \( \tau \) is the Salem number of degree \( 2s \), then the integers of \( Q(\tau) \), namely \( 1, \tau, \ldots, \tau^{2s-1} \) form a base of \( Q(\tau) \) over \( Q \). We denote \( \Delta_\tau \) the discriminant of that base, that is
Let \( \gamma \) be a Salem number, then there exists a non zero integer \( c \) such that

\[
\Delta_\gamma = c \cdot \left( \Delta_{\gamma+\frac{1}{\tau}} \right)^2.
\]

**PROOF.**

By definition,

\[
\Delta_\gamma = (\tau - \frac{1}{\tau})^2 \prod_{j=2}^s (\tau - \tau(j))^2 (\tau - \frac{1}{\tau(j)})^2 \prod_{j=2}^s \left( \frac{1}{\tau} - \tau(j) \right)^2
= \prod_{i<j} (\tau_i - \tau_j)^2,
\]

where \( \tau = \tau_1, \tau_2 = \frac{1}{\tau}, \tau_3 = \tau(2), \tau_4 = \frac{1}{\tau(2)}, \ldots, \tau_{2s} = \frac{1}{\tau(2s)} \).

The totally real number field \( \mathbb{Q}(\tau + \frac{1}{\tau}) \) has also a base of algebraic integers \( 1, \tau + \frac{1}{\tau}, \ldots, (\tau + \frac{1}{\tau})^{s-1} \) with discriminant

\[
\Delta_{\tau+\frac{1}{\tau}} = \left| \begin{array}{cccc}
1 & 1 & (\tau(2)) & \cdots \\
\frac{1}{\tau} & \frac{1}{\tau(2)} & \cdots \frac{1}{\tau(2)}
\end{array} \right| = \prod_{i<j} (\gamma_i - \gamma_j)^2,
\]

where \( \gamma_1 = \tau + \frac{1}{\tau}, \gamma_2 = \tau(2) + \frac{1}{\tau(2)}, \ldots, \gamma_s = \tau(s) + \frac{1}{\tau(s)} \).

**Proposition 13.** Let \( \tau \) be a Salem number, then there exists a non zero integer \( c \) such that

\[
\Delta_\gamma = c \cdot \left( \Delta_{\gamma+\frac{1}{\tau}} \right)^2.
\]
Lemma 14. Let \( \tau \) be a Salem number and denote \( \tau = \alpha_1, ..., \alpha_d \) the conjugates of a Salem number \( \tau \). Then \( \tau^p = \alpha_1^p, ..., \alpha_d^p \) are the conjugates of the Salem number \( \tau^p \) and we get the inequality

\[
\prod_{i,j} (\alpha_i^p - \alpha_j) \geq p^d.
\]

PROOF. Let \( P \) (resp. \( \Pi \)) denote the minimal polynomial of the Salem \( \tau \) (resp. \( \tau^p \)) and \( A = \prod_{i,j} (\alpha_i^p - \alpha_j) \).

We observe that \( A \neq 0 \), otherwise \( P \) and \( \Pi \) would have a common root and since they are monic and irreducible, \( P = \Pi \), a contradiction.

Moreover \( A \) being a symmetric function of the \( \alpha_i \) is an integer, nothing else than the resultant of \( P \) and \( \Pi \).

First, given a polynomial \( Q \in \mathbb{Z}[X] \), we prove the existence of a polynomial \( R(X) \in \mathbb{Z}[X] \) satisfying

\[
(Q(X))^p = Q(X^p) + pR(X).
\]

We make an induction on the degree of \( Q \).

If the degree of \( Q \) is 1, that is \( Q = aX + b \), \( a \) and \( b \in \mathbb{Z} \), we obtain

\[
(aX + b)^p = a^pX^p + b^p + pR_1(X), \quad R_1 \in \mathbb{Z}[X]
\]

From the little Fermat’s theorem, since \( a^p \equiv a \mod p \) and \( b^p \equiv b \mod p \), we get

\[
(aX + b)^p = aX^p + b + (a^p - a)X^p + b^p - b + pR_1(X)
= aX^p + b + pR(X), \quad R \in \mathbb{Z}[X].
\]

Suppose the relation satisfied until degree \( n \) and suppose that the degree of \( Q \) is \( n + 1 \).

Write \( Q(X) = XQ_1(X) + c \) with \( c \in \mathbb{Z} \) and degree of \( Q_1 \) being \( n \). We get

\[
(XQ_1(X) + c)^p = X^p(Q_1(X))^p + c^p + pR_1(X), \quad R_1 \in \mathbb{Z}[X]
= X^p(Q_1(X^p) + pR_2(X)) + c^p + pR_1(X) \quad R_2 \in \mathbb{Z}[X]
\text{by induction}
= X^pQ_1(X^p) + c + c^p - c + p(R_1(X) + X^pR_2(X))
= Q(X^p) + pR(X) \quad R \in \mathbb{Z}[X]
\]

using again little Fermat’s theorem.

Taking now \( Q = P = (X - \alpha_1)...(X - \alpha_d) \), it follows

\[
P(\alpha_i^p) = -pR(\alpha_i) \neq 0
\]
and
\[ |A| = \prod \left| P(\alpha_i^p) \right| = p^d \prod \left| R(\alpha_i) \right| \geq p^d, \]
since, \( \prod_i R(\alpha_i) \), symmetric function of the \( \alpha_i \), is a rational integer. \( \square \)

**Theorem 15.** (Bertin [Be95]) Let \( \tau \) be a Salem number of degree \( d = 2s \); then
\[ \tau \geq 1 + \inf \left( \frac{|\Delta_{\tau + \frac{1}{\tau}}|^{1/s}}{96s}, 1/6 \right). \]

**PROOF.** Let \( p \) denote a prime number and \( \tau = \alpha_1, \alpha_2, \ldots, \alpha_d \) the conjugates of the Salem number \( \tau \). Consider the determinant
\[
D = \begin{vmatrix}
1 & 1 & \ldots & 1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \ldots & \alpha_d & \alpha_1^p & \ldots & \alpha_d^p \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\alpha_1^{2d-1} & \alpha_2^{2d-1} & \ldots & \alpha_d^{2d-1} & \alpha_1^{p(2d-1)} & \ldots & \alpha_d^{p(2d-1)}
\end{vmatrix}
\]

We can write
\[ |D|^2 = \prod_{i \neq j} |\alpha_i - \alpha_j| \prod_{i \neq j} |\alpha_i^p - \alpha_j^p| \prod_{i,j} |\alpha_i^p - \alpha_j| \]

Then, from the lemma and the proposition, it follows
\[ |D|^2 \geq |\Delta_{\tau}||\Delta_{\tau^p}|p^{2d} \geq |\Delta_{\tau^2}|p^{2d} \geq |\Delta_{\tau+1/\tau}|^{1/s}p^{2d}. \]

By Hadamard’s inequality applied to the columns of \( D \), we get
\[ |D|^2 \leq 2d\tau^{2(2d-1)}(2d)^{d-1}2d\tau^{2p(2d-1)}(2d)^{d-1} \leq (2d)^{2d}\tau^{2(2d-1)(p+1)} \leq (2d)^{2d(p+1)}2d. \]

From the previous majoration and minoration of \( |D| \), we obtain
\[ |\Delta_{\tau+1/\tau}|^{1/s}p^{2d} \leq (2d)^{2d(p+1)}2d \]
that is
\[ \tau^{2(p+1)} \geq \frac{p}{2d} |\Delta_{\tau+1/\tau}|^{2/d} = \frac{p}{2d} |\Delta_{\tau+1/\tau}|^{1/s}. \]

Now we choose the prime number \( p \) as best as possible. By Bertrand’s lemma, given a rational integer \( m \in \mathbb{N} \), there exists a prime number \( m \leq p \leq 2m \). Thus we can choose \( p \) such that
\[ \frac{6d}{|\Delta_{\tau+1/\tau}|^{1/s}} < \left[ \frac{6d}{|\Delta_{\tau+1/\tau}|^{1/s}} \right] + 1 \leq p \leq 2 \left[ \frac{6d}{|\Delta_{\tau+1/\tau}|^{1/s}} \right] + 2, \]
where \([x]\) denotes the integer part of \( x \). We deduce
\[ \frac{p}{2d} |\Delta_{\tau+1/\tau}|^{1/s} > 3 > e; \]
thus
\[ \tau^{2(p+1)} > e \quad \text{et} \quad \tau > 1 + \frac{1}{2(p+1)}. \]
If \( \frac{6d}{|\Delta_{r+1}/r|^{1/s}} < 1 \), we take \( p = 2 \), thus \( \tau > 1 + 1/6 \); otherwise \( 12s \geq \frac{|\Delta_{r+1}/r|^{1/s}}{\tau} \) and \( p \leq \frac{12d}{|\Delta_{r+1}/r|^{1/s}} + 1 \). Thus

\[
\tau > 1 + \frac{|\Delta_{r+1}/r|^{1/s}}{96s}.
\]

This achieves the proof of the theorem.

\[\square\]

**Remark 16.** This result shows, in Lehmer’s question, the importance of the quantity \( |\Delta_{r+1}/r|^{1/s} \). The minoration by \( \frac{2^{1/d}}{\delta_d} \), where \( \delta_d \) denotes the smallest totally real discriminant of degree \( d \), is not interesting, since a result of Martinet only asserts that for \( d \) large, \( \Delta_{r+1}^{1/d} < 1085 \). However, trace polynomials of Salem polynomials are very peculiar totally real polynomials since we have seen that the roots are in a sense well distributed. I evaluated \( \Delta_{d}^{1/d} \) for the list of known small Salem numbers and found that this quantity varies between \( 1.4299 \) for \( \sigma_{34} \) of degree 18 and \( 2.27134 \) for \( \sigma_{8} \) of degree 20.

**References**

[Pi17] T. Pierce, The numerical factors of the arithmetic funtions \( \prod_{i=1}^{n}(1 \pm \alpha_i) \), *Ann. of Math.* **18** (1916-17).

Marie-José Bertin: Université Pierre et Marie Curie (Paris 6), Institut de Mathématiques, 4 Place Jussieu, 75005 Paris, France

E-mail address: bertin@math.jussieu.fr