Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Artūras DUBICKAS et Jonas JANKAUSKAS

Linear relations with conjugates of a Salem number

Tome 32, n[o] 1 (2020), p. 179-191.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2020__32_1_179_0>

Journal de Théorie des Nombres de Bordeaux **32** (2020), 179–191

Linear relations with conjugates of a Salem number

par Artūras DUBICKAS et Jonas JANKAUSKAS

Résumé. Dans cet article, nous considérons les relations linéaires entre les conjugués d'un nombre de Salem α. Nous montrons qu'une telle relation provient d'une relation linéaire entre les conjugués de l'entier algébrique totalement réel correspondant $\alpha + 1/\alpha$. On montre également que le plus petit degré d'un nombre de Salem satisfaisant à une relation non triviale entre ces conjugués est 8 tandis que la longueur la plus courte d'une relation linéaire non-triviale entre les conjugués d'un nombre de Salem est 6.

Abstract. In this paper we consider linear relations with conjugates of a Salem number α. We show that every such a relation arises from a linear relation between conjugates of the corresponding totally real algebraic integer $\alpha + 1/\alpha$. It is also shown that the smallest degree of a Salem number with a nontrivial relation between its conjugates is 8, whereas the smallest length of a nontrivial linear relation between the conjugates of a Salem number is 6.

1. Introduction

Let α be an algebraic number of degree $d \geq 2$ over $\mathbb{Q}$ with conjugates $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$. An additive linear relation

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_d\alpha_d = 0 \tag{1.1}$$

with some $k_1, k_2, \dots, k_d \in \mathbb{Q}$ is called *nontrivial* if $k_i \neq k_j$ for some $1 \leq i < j \leq d$. Thus, the relation

$$\mathrm{Trace}(\alpha) := \alpha_1 + \alpha_2 + \cdots + \alpha_d = 0$$

and its rational multiples $\sum_{j=1}^{d} r\alpha_j = 0$, where $r \in \mathbb{Q}$, are *trivial* linear relations. (These hold for conjugates of any algebraic number whose trace is zero.) Note that if (1.1) is a nontrivial linear relation with some

Manuscrit reçu le 10 mai 2019, révisé le 26 mai 2019, accepté le 13 juillet 2019.

2020 *Mathematics Subject Classification.* 11R06, 11R09.

Mots-clefs. linear additive relations, Salem numbers, Pisot numbers, totally real algebraic numbers.

We thank the referee for pointing out some inaccuracies. The research of the first named author was funded by the European Social Fund according to the activity "Improvement of researchers" qualification by implementing world-class R&D projects of Measure No. 09.3.3-LMT-K-712-01-0037. The post-doctoral position of the second named author is supported by the Austrian Science Fund (FWF) project M2259 Digit Systems, Spectra and Rational Tiles under the Lise Meitner Program.

$k_1, k_2, \dots, k_d \in \mathbb{Q}$ then, by multiplying all the k_i by their common denominator, we can assume that $k_1, k_2, \dots, k_d \in \mathbb{Z}$. Accordingly, we call the sum

$$|k_1| + |k_2| + \cdots + |k_d| \in \mathbb{N}$$

the *length* of the relation (1.1).

The investigation of nontrivial linear relations (1.1) in conjugates of algebraic numbers has begun with the papers of Kurbatov [16, 17, 18]. In [26], Smyth obtained some useful results and also formulated several natural conjectures on the possibility of (1.1) which are still wide open; see also his previous paper [25]. Further results on this subject have been obtained by several authors in [1, 5, 6, 7, 8, 9, 15, 19, 20, 28].

Recently, in [10] it was shown that there is a unique Pisot number $\alpha = (1 + \sqrt{3 + 2\sqrt{5}})/2$ with minimal polynomial $x^4 - 2x^3 + x - 1$ satisfying the nontrivial linear relation

$$\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 = 0$$

of length 4. Recall that an algebraic integer $\alpha > 1$ is called a *Pisot number* if its other conjugates over $\mathbb{Q}$ (if any) all lie in the open unit disc $|z| < 1$. This answers two questions raised earlier in [12]. For instance, this implies that no two conjugates of a Pisot number can have the same imaginary part. See also a subsequent paper [11] for some further analysis of some simple linear relations of small length.

In the present paper, we investigate additive linear relations in conjugates of a Salem number. Recall that an algebraic integer $\alpha > 1$ is called a *Salem number* if its other conjugates over $\mathbb{Q}$ all lie in the closed unit disc $|z| \leq 1$ with at least one conjugate lying on the circle $|z| = 1$. Of course, this implies that $1/\alpha$ is a conjugate to α, whereas all other conjugates lie on the circle $|z| = 1$.

Throughout, if $\alpha > 1$ is a Salem number of degree $d = 2s \geq 4$ we label its conjugates as in the theorem below.

Theorem 1.1. *Let $\alpha_1 = \alpha > 1$ be a Salem number of degree $d = 2s \geq 4$ with conjugates $\alpha_1, \dots, \alpha_d$ satisfying $\alpha_2 = 1/\alpha_1$ and $\alpha_{2j} = 1/\alpha_{2j-1} = \overline{\alpha_{2j-1}}$ for $j = 2, \dots, s$. If for some rational numbers k_i, $i = 1, \dots, d$, and for some totally real algebraic number γ we have*

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_d\alpha_d = \gamma, \tag{1.2}$$

then $k_{2j-1} = k_{2j}$ for each $j = 1, \dots, s$.

In particular, the theorem obviously holds for $\gamma = 0$. So, every linear relation (1.1) in the conjugates α_i, $i = 1, \dots, d$, of a Salem number α is induced by the linear relation

$$k_1\beta_1 + k_3\beta_2 + \cdots + k_{2s-1}\beta_s = 0 \tag{1.3}$$

in conjugates of the respective totally real algebraic integer $\beta_1 = \beta :=$ $\alpha + 1/\alpha > 2$ whose other conjugates are

$$\beta_j = \alpha_{2j-1} + \alpha_{2j} = \alpha_{2j-1} + 1/\alpha_{2j-1} = \alpha_{2j-1} + \overline{\alpha_{2j-1}} = 2\Re\alpha_{2j-1} \in (-2, 2)$$

for $j = 2, \dots, s$. If f is the minimal polynomial of a Salem number α of degree $d = 2s$ and g is the minimal polynomial of $\beta = \alpha + 1/\alpha$ of degree s then they are related by the identity $f(x) = x^s g(x + 1/x)$. Then, as in [4], we call g the *trace polynomial* of f. Note that f is irreducible if and only if g is irreducible. Also, $\mathrm{Trace}(\alpha) = \sum_{j=1}^{d} \alpha_j = \sum_{i=1}^{s} \beta_i = \mathrm{Trace}(\beta)$.

By [18] (or [6]), the only relation with conjugates $\beta_1 = \beta, \dots, \beta_p$ of an irreducible polynomial of prime degree p can be of the form

$$r\beta_1 + r\beta_2 + \cdots + r\beta_p = 0,$$

where $r \in \mathbb{Q}$. Hence, the only possible linear relation with conjugates of a Salem number α with degree $2p$ is $r\,\mathrm{Trace}(\alpha) = 0$, where $r \in \mathbb{Q}$. This relation is trivial.

So, in particular Theorem 1.1 implies that

Corollary 1.2. *If p is a prime number then there are no nontrivial linear relations in conjugates of a Salem number of degree $d = 2p$.*

By [21], it is known that there are Salem numbers of every integral trace. The degree of a Salem number with negative trace $-t$ is quite large if $t \in \mathbb{N}$ is large. Earlier, in [27] Smyth has shown that there are Salem numbers with trace -1 of every even degree $d \geq 8$.

Here, by a similar argument, we show that

Theorem 1.3. *For every even $d \geq 6$ there is a Salem number of degree d with trace* 0*.*

In Corollary 2.2 below, we list of all 4 possible Salem numbers of degree 6 and trace 0. Note that there are no Salem numbers of degree 4 and trace 0. Indeed, otherwise the minimal polynomial of such a Salem number would be $x^4 + ax^2 + 1$, with $a \in \mathbb{Z}$, which is impossible, since $-\alpha$ is not a conjugate of a Salem number α.

Our next theorem describes the minimal length of nontrivial linear relations between conjugates of a Salem number and the minimal degree of a Salem number for which a nontrivial linear relation may occur.

Theorem 1.4. *Suppose $\alpha > 1$ is a Salem number with conjugates $\alpha_1 =$ $\alpha, \alpha_2, \dots, \alpha_d$ over $\mathbb{Q}$ labelled as in Theorem 1.1.*

(i) *If for some integers $k_1, k_2, \dots, k_d$, not all zero, the nontrivial linear relation* (1.1) *holds then its length must be at least* 6*. Furthermore, there exist Salem numbers α of degree* 12 *whose conjugates can be* *labelled so that they satisfy the following nontrivial linear relation of length* 6*:*

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 = \sum_{j=1}^{6} 1 \cdot \alpha_j + \sum_{j=7}^{12} 0 \cdot \alpha_j = 0.$$

(ii) *The smallest degree of a Salem number with a nontrivial linear relation between its conjugates is* 8*. Furthermore, there exist Salem numbers* α *of degree* 8 *whose conjugates can be labelled so that they satisfy the following nontrivial linear relation:*

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 - \alpha_5 - \alpha_6 - \alpha_7 - \alpha_8 = 0.$$

In the next section we will give some auxiliary results. Then, in Section 3 we will prove the theorems.

2. Auxiliary results

We begin with two simple lemmas.

Lemma 2.1. *The cubic polynomial* $x^3 - ax + b \in \mathbb{R}[x]$ *has three distinct roots in the interval* $(-2, 2)$ *if and only if* $0 < a < 4$ *and*

$$\max\left(2a - 8, -\frac{2a\sqrt{a}}{3\sqrt{3}}\right) < b < \min\left(8 - 2a, \frac{2a\sqrt{a}}{3\sqrt{3}}\right). \tag{2.1}$$

It has two distinct roots in $(-2, 2)$ *and one root in* $(2, +\infty)$ *if and only if* $3 < a < 12$ *and*

$$-\frac{2a\sqrt{a}}{3\sqrt{3}} < b < -|2a - 8|. \tag{2.2}$$

Note that (2.1) implies $2a - 8 < b$, whereas (2.2) yields $b < 2a - 8$.

Proof. Set

$$h(x) := x^3 - ax + b.$$

Since $h'(x) = 3x^2 - a$, the polynomial h has only one real root if $a \le 0$.

Suppose $a > 0$. Set $x_0 := \sqrt{a/3}$. Then, the polynomial h has three distinct roots in $(-2, +\infty)$ iff $-2 < -x_0$ (i.e., $0 < a < 12$),

$$h(-2) = -8 + 2a + b < 0, \tag{2.3}$$

$$h(-x_0) = \frac{2a\sqrt{a}}{3\sqrt{3}} + b > 0 \tag{2.4}$$

and

$$h(x_0) = -\frac{2a\sqrt{a}}{3\sqrt{3}} + b < 0. \tag{2.5}$$

Clearly, all three roots belong to $(-2, 2)$ if, in addition, we have $h(2) = 8 - 2a + b > 0$. Combined with (2.3), (2.4) and (2.5) this proves (2.1).

Evidently, (2.1) is only possible for some b when its left hand side does not exceed its right hand side, that is, when $0 < a < 4$.

Similarly, two roots of h are in $(-2, 2)$ and one root in $(2, +\infty)$ when one has (2.3), (2.4), and $h(2) = 8 - 2a + b < 0$. (As h is increasing in the interval $(x_0, 2)$, the inequality (2.5) automatically holds.) Evidently, all these inequalities combine into (2.2). Here, as $0 < a < 12$, it is easy to see that the inequality

$$|2a - 8| < \frac{2a\sqrt{a}}{3\sqrt{3}}$$

holds only for a in the range $3 < a < 12$, so only for such a one can find some b satisfying (2.2). $\square$

Observe that there are only 7 pairs of integers (a, b) satisfying the conditions $3 < a < 12$ and (2.2), namely, $(4, -1)$, $(4, -2)$, $(4, -3)$, $(5, -3)$, $(5, -4)$, $(6, -5)$ and $(7, -7)$. However, the polynomials $x^3 - 4x - 3$, $x^3 - 5x - 4$ and $x^3 - 6x - 5$ are reducible. The other four polynomials $x^3 - 4x - 1$, $x^3 - 4x - 2$, $x^3 - 5x - 3$ and $x^3 - 7x - 7$ are irreducible. So, Lemma 2.1 implies that

Corollary 2.2. *There are exactly four Salem numbers of degree* 6 *with trace* 0*. Their minimal polynomials are:*

$$x^6 - x^4 - x^3 - x^2 + 1, \quad x^6 - x^4 - 2x^3 - x^2 + 1,$$
$$x^6 - 2x^4 - 3x^3 - 2x^2 + 1, \quad x^6 - 4x^4 - 7x^3 - 4x^2 + 1.$$

Lemma 2.3. *Let $h(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $k \geq 2$ with $k - 1$ roots in the interval $(-2, 1/4)$ and one root in $(-6, -2)$. Then,*

$$f(x) := (-1)^k x^{2k} h\big((x + 1/x)(1 - x - 1/x)\big) \in \mathbb{Z}[x]$$

is a monic reciprocal polynomial of degree $4k$ which defines a Salem number of degree $d = 4k$ in case it is irreducible over $\mathbb{Q}$. Moreover, the conjugates of this Salem number α can be labelled so that

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = \cdots = \alpha_{4k-3} + \alpha_{4k-2} + \alpha_{4k-1} + \alpha_{4k} = 1. \tag{2.6}$$

Proof. Let $\gamma_1 \in (-6, -2)$ and $\gamma_2 < \cdots < \gamma_k \in (-2, 1/4)$ be the roots of h. Consider the monic polynomial $g(x) := (-1)^k h(x(1 - x))$. Then, its roots

$$\beta_{2j-1} := \frac{1 + \sqrt{1 - 4\gamma_j}}{2} \quad \text{and} \quad \beta_{2j} := \frac{1 - \sqrt{1 - 4\gamma_j}}{2}, \tag{2.7}$$

where $j = 1, \dots, k$, satisfy

$$\beta_1 = (1 + \sqrt{1 - 4\gamma_1})/2 > 2,$$
$$\beta_2 = (1 - \sqrt{1 - 4\gamma_1})/2 \in (-2, -1)$$

and $\beta_3, \dots, \beta_{2k} \in (-1, 2)$. So, g has $2k - 1$ roots in $(-2, 2)$ and one root greater than 2. Clearly, by (2.7), we have

$$\beta_1 + \beta_2 = \cdots = \beta_{2k-1} + \beta_{2k} = 1. \tag{2.8}$$

Now, as the roots $\alpha_1 = \alpha > 1, \alpha_2 = 1/\alpha, \dots, \alpha_{4k-1}, \alpha_{4k} = 1/\alpha_{4k-1}$ of

$$f(x) = x^{2k} g(x + 1/x) = (-1)^k x^{2k} h\big((x + 1/x)(1 - x - 1/x)\big)$$

satisfy $\beta_j = \alpha_{2j-1} + \alpha_{2j} = \alpha_{2j-1} + 1/\alpha_{2j-1}$ for each $j = 1, \dots, 2k$, we see that (2.8) implies (2.6). Furthermore, α is a Salem number of degree $4k$ provided that f is irreducible over $\mathbb{Q}$. $\square$

We made some calculations related to Lemma 2.3. It turns out that there exactly 15 quadratic polynomials h satisfying the conditions of the lemma and thus producing 15 Salem numbers of degree 8 satisfying (2.6) with $k = 2$. For instance, $x^2 + 4x + 1$ is such a quadratic polynomial h. Also, there are exactly 30 cubic, 20 quartic and 4 quintic polynomials h producing 30 Salem numbers of degree 12 (satisfying (2.6) with $k = 3$), 20 Salem numbers of degree 16 (satisfying (2.6) with $k = 4$) and 4 Salem numbers of degree 20 (satisfying (2.6) with $k = 5$), respectively. In the case $k = 5$, the example of h is

$$x^5 + 9x^4 + 22x^3 + 16x^2 - x - 1.$$

This gives a Salem number α of degree 20 with minimal polynomial

$$x^{20} - 5x^{19} + 11x^{18} - 19x^{17} + 26x^{16} - 29x^{15} + 27x^{14} - 19x^{13} + 8x^{12} + x^{11}$$
$$- 5x^{10} + x^9 + 8x^8 - 19x^7 + 27x^6 - 29x^5 + 26x^4 - 19x^3 + 11x^2 - 5x + 1$$

whose conjugates satisfy (2.6) with $k = 5$.

The first part of the next lemma was inspired by Lemma 1 of Beukers and Smyth in [2]. Essentially, it is a version of their algorithm [2] to locate cyclotomic points on curves, specialized to the case of sequences of polynomials that produce Salem numbers from Pisot numbers. Also, the second part of Lemma 2.4 is loosely related to the work on irreducibility of polynomials of the type $x^n f(x) + g(x) \in \mathbb{Z}[x]$ and on the sequences and covering systems of integers by Schinzel [24], Filaseta et al. [13, 14], although these irreducibility results are not of direct relevance here. Throughout, $f^*(x) = x^{\deg f} f(1/x)$ stands for the *reciprocal polynomial* of $f(x)$.

Lemma 2.4. *For $n \in \mathbb{N}$, consider the sequence of polynomials*

$$g_n(x) := x^n f(x) + \varepsilon f^*(x),$$

where $\varepsilon \in \{-1, 1\}$ and $f(x) \in \mathbb{Z}[x]$ satisfies $f^*(x) \neq \pm f(x)$. Suppose that a root of unity $\zeta \in \mathbb{C}$ is also a root of some polynomial $g_n(x)$. Then, ζ must appear among the zeros of at least one of the following polynomials:

$$f(x^2) f^*(x)^2 + \varepsilon f(x)^2 f^*(x^2), \qquad f(x)^2 f^*(-x^2) \pm f(-x^2) f^*(x)^2,$$
$$f(x) f^*(-x) \pm f(-x) f^*(x).$$

In particular, if none of these polynomials is identically zero, then the set of all such possible roots of unity ζ is finite.

In addition, if $f(\zeta) \neq 0$ *then the root of unity* ζ *is a zero of* $g_n(z)$ *if and only if* n *belongs to the arithmetic progression* $\ell k + r$, $k = 0, 1, 2, \dots$, *where* r *is a fixed integer in the range* $0 \leq r < \ell$ *and* $\ell = \mathrm{ord}(\zeta)$ *denotes the multiplicative order of* ζ.

Proof. As ζ is the root of unity, by Lemma 1 of [2] (or Lemma 2.1 of [27]), at least one of the three numbers ζ^2, $-\zeta^2$, $-\zeta$ must be an algebraic conjugate of ζ over $\mathbb{Q}$. Multiplying $g_n(x) = x^n f(x) + \varepsilon f^*(x)$ by $x^n f(x) - \varepsilon f^*(x)$ we see that the polynomial $h(x) = x^{2n} f(x)^2 - f^*(x)^2$ has a zero at $x = \zeta$.

If ζ^2 is conjugate of ζ, then one also has $g_n(\zeta^2) = 0$. Combining this with $h(\zeta) = 0$ yields

$$\begin{cases} \zeta^{2n} f(\zeta)^2 - f^*(\zeta)^2 & = 0, \\ \zeta^{2n} f(\zeta^2) + \varepsilon f^*(\zeta^2) & = 0. \end{cases}$$

Hence,

$$\begin{vmatrix} f(\zeta)^2 & -f^*(\zeta)^2 \\ f(\zeta^2) & \varepsilon f^*(\zeta^2) \end{vmatrix} = \varepsilon f(\zeta)^2 f^*(\zeta^2) + f(\zeta^2) f^*(\zeta)^2 = 0.$$

Thus, ζ is the root of

$$f(x^2) f^*(x)^2 + \varepsilon f(x)^2 f^*(x^2).$$

Suppose next that $-\zeta^2$ is a conjugate to ζ. Then, using $g_n(-\zeta^2) = 0$ and $h(\zeta) = 0$, one concludes that ζ is the root of the polynomial

$$f(x)^2 f^*(-x^2) + \varepsilon(-1)^n f(-x^2) f^*(x)^2.$$

In the case when $-\zeta$ is conjugate to ζ, from $g_n(\zeta) = g_n(-\zeta) = 0$ one obtains $\zeta^n f(\zeta) + \varepsilon f^*(\zeta) = 0$ and $(-\zeta)^n f(-\zeta) + \varepsilon f^*(-\zeta) = 0$, which yields that ζ is a root of

$$f(x) f^*(-x) + (-1)^{n+1} f(-x) f^*(x).$$

Finally, if a root of unity ζ of order ℓ satisfies $g_n(\zeta) = 0$, then $g_{n+\ell}(\zeta) = 0$. Furthermore, if ζ is a common root of $x^{n_1} f(x) + \varepsilon f^*(x)$ and $x^{n_2} f(x) + \varepsilon f^*(x)$, then $(\zeta^{n_2} - \zeta^{n_1}) f(\zeta) = (\zeta^{n_2 - n_1} - 1)\zeta^{n_1} f(\zeta) = 0$. By $f(\zeta) \neq 0$, it follows that $\zeta^{n_2 - n_1} = 1$. Thus, $\ell \mid (n_2 - n_1)$ and so all such n form an arithmetic progression with difference ℓ, as claimed. □

3. Proofs of the theorems

Proof of Theorem 1.1. Assume that $k_{2i} \neq k_{2i-1}$ for some i in the range $1 \leq i \leq s$. Let G be the Galois group of the normal extension of $\mathbb{Q}(\alpha, \gamma)$ over $\mathbb{Q}$, and let σ be an automorphism of G which maps α_{2i-1} to $\alpha_1 = \alpha$. Then, $\sigma(\alpha_{2i}) = \sigma(1/\alpha_{2i-1}) = 1/\alpha$, so that (1.2) maps into

$$\sigma(\gamma) = k_{2i-1}\alpha + k_{2i}/\alpha + t_3\alpha_3 + \dots + t_d\alpha_d, \tag{3.1}$$

where $t_3, \dots, t_d \in \mathbb{Q}$ is a permutation of the list obtained from the initial list $k_1, \dots, k_d$ by excluding the elements k_{2i-1} and k_{2i}.

Consider the following equality which is complex conjugate to (3.1):

$$\overline{\sigma(\gamma)} = k_{2i-1}\alpha + k_{2i}/\alpha + t_3\overline{\alpha_3} + \dots + t_d\overline{\alpha_d}. \tag{3.2}$$

Since $\overline{\sigma(\gamma)} = \sigma(\gamma)$ and $\alpha_{2j} = \overline{\alpha_{2j-1}}$ for $j = 2, \dots, s$, by adding (3.1) and (3.2), we obtain

$$2\sigma(\gamma) = 2k_{2i-1}\alpha + 2k_{2i}/\alpha + w_2(\alpha_3 + \alpha_4) + \dots + w_s(\alpha_{d-1} + \alpha_d),$$

where $w_j = t_{2j-1} + t_{2j}$ for $j = 2, 3, \dots, s$. Adding $2(k_{2i} - k_{2i-1})\alpha$ to both sides we deduce that

$$2\sigma(\gamma) + 2(k_{2i} - k_{2i-1})\alpha = w_1(\alpha_1 + \alpha_2) + w_2(\alpha_3 + \alpha_4) + \dots + w_s(\alpha_{d-1} + \alpha_d),$$

where $w_1 = 2k_{2i}$.

As we already observed above, the number $\beta_1 = \beta = \alpha + 1/\alpha = \alpha_1 + \alpha_2$ is totally real with conjugates $\beta_2 = \alpha_3 + \alpha_4, \dots, \beta_s = \alpha_{d-1} + \alpha_d$. Hence, the number

$$2(k_{2i} - k_{2i-1})\alpha = w_1\beta_1 + w_2\beta_2 + \dots + w_s\beta_s - 2\sigma(\gamma)$$

is a linear form (with rational coefficients $w_1, \dots, w_s, -2$) in totally real algebraic numbers $\beta_1, \dots, \beta_s, \sigma(\gamma)$. Thus, it must be totally real itself. However, the number $2(k_{2i} - k_{2i-1})\alpha \neq 0$ is not totally real, since it has a non-real conjugate $2(k_{2i} - k_{2i-1})\alpha_3$. This is a contradiction which completes the proof of the theorem. $\square$

Proof of Theorem 1.3. Assume that there exists a smallest even degree d (where $d \geq 8$ by Corollary 1.3), such that there are no Salem numbers of that degree d with trace 0. We will track down and ultimately eliminate all such possible d by considering 3 sequences of polynomials, given explicitly by Salem's original construction [22, 23].

We start with a Salem sequence

$$g_n(x) = x^n(x^3 - x - 1) + (-x^3 - x^2 + 1), \quad n \geq 2.$$

Then $g_n(x)$ either posseses cyclotomic factors or it is a minimal polynomial of a Salem number of trace 0; see [3, 22, 23]. Since we have assumed that no Salem number of degree d and trace 0 exists, the polynomial $g_n(x)$ of degree $d = \deg g_n = n + 3$ must be reducible, that is, it must be divisible by a cyclotomic polynomial $\Phi_\ell(x)$, where $\ell \in \mathbb{N}$.

To find cyclotomic factors of $g_n(x)$, we apply Lemma 2.4 with $f(x) = x^3 - x - 1$ and $\varepsilon = 1$. The following candidates appear as factors of auxiliary polynomials described in Lemma 2.4 (with $\varepsilon = 1$):

$$\Phi_1(x) = x - 1, \qquad \Phi_2(x) = x + 1, \qquad \Phi_8(x) = x^4 + 1$$

$$\Phi_{12}(x) = x^4 - x^2 + 1, \qquad \Phi_{18}(x) = x^6 - x^3 + 1,$$

$$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$$

Since none of the five auxiliary polynomials is zero identically, this list is complete.

To see which of these candidates actually show up, one can apply the periodicity property stated in the second part of Lemma 2.4. After computation of $\gcd(g_n(x), \Phi_\ell(x))$, $0 \le n \le \ell - 1$, for $\ell = 1, 2, 8, 12, 18, 30$ it turns out that $g_n(x)$ has cyclotomic factors precisely for the degrees $d = n+3$ in one of the following arithmetic progressions

$$d \in \{2k+1, 8k+2, 12k+1, 18k+17, 30k+24\},$$

where $k = 0, 1, 2, \ldots$. As d must be even, we restrict all such possible d to two arithmetic progressions: $d \in \{8k+2, 30k+24\}$.

Next, we take the second sequence

$$h_n(x) = \frac{x^n(x^2 - x - 1) - (-x^2 - x + 1)}{x - 1}, \quad n \ge 2.$$

Although now $f(x) = x^2 - x - 1$ contributes the coefficient -1 of x^{n+1} to $g_n(x)$, one regains trace 0 after division by $x - 1$. Let us apply Lemma 2.4 to the polynomial $g_n(x) = (x-1)h_n(x)$ with this new choice of $f(x)$ and $\varepsilon = -1$. The candidate cyclotomic factors are:

$$\Phi_1(x) = x - 1, \qquad \Phi_2(x) = x + 1, \qquad \Phi_3(x) = x^2 + x + 1,$$
$$\Phi_6(x) = x^2 - x + 1, \qquad \Phi_{12}(x) = x^4 - x^2 + 1.$$

As above, the computation of gcd's with first 12 polynomials of the sequence yields the list of possible bad degrees $d = n + 1$:

$$d \in \{2k+1, 3k+2, 6k+3, 12k+4\}.$$

This list also accounts for the single occurrence of the multiple factors, namely, $(x-1)^2$ in $g_4(x)$. Bad degrees must be even, so we are left with $d \in \{6k+2, 12k+4\}$.

Let us combine this with the arithmetic progressions obtained from the first sequence:

$$d \in \{8k+2, 30k+24\} \cap \{6k+2, 12k+4\}.$$

Notice that all integers $30k+24$ are divisible by 6, while none of $6k+2$ or $12k+4$ are. Therefore, $d \notin \{30k+24\}$, and hence $d \in \{8k+2\}$. Next, notice that $12k+4$ is divisible by 4 while $8k+2$ is not. Consequently, $d \notin \{12k+4\}$. It follows that

$$d \in \{8k+2\} \cap \{6k+2\} = \{24k+2\}.$$

To eliminate this possibility, let us consider the third sequence, constructed with $f(x) = x^3 - x^2 - 1$ and $\varepsilon = -1$:

$$h_n(x) = \frac{x^n(x^3 - x^2 - 1) - (-x^3 - x + 1)}{x - 1}, \quad n \ge 2.$$

This time, by Lemma 2.4, the candidates for cyclotomic divisors are

$\Phi_1(x) = x-1, \quad \Phi_2(x) = x+1, \quad \Phi_3(x) = x^2+x+1, \quad \Phi_4(x) = x^2+1,$

$\Phi_6(x) = x^2-x+1, \quad \Phi_{10}(x) = x^4-x^3+x^2-x+1, \quad \Phi_{18}(x) = x^6-x^3+1.$

Now, bad degrees $d = n+2$ for this sequence $h_n(x)$ are

$$d \in \{2k+1, 3k+1, 4k+3, 6k+4, 10k+5, 18k+6\}.$$

This last list accounts for the factor $(x-1)^2$ of $g_5(x)$ for a single value $n = 5$. Since d is even, $d \notin \{2k+1, 4k+3, 10k+5\}$. Since $d \in \{24k+2\}$ has remainder 2 (mod 3), we deduce that $d \notin \{3k+1, 6k+4\}$. Finally, $d \notin \{18k+6\}$, since $24k+2$ is not divisible by 6. This exhausts the list of possibilities, so no such bad degrees can exist. Hence, for each even $d \geq 6$, we can find a Salem number of degree d and trace 0 in one of the three Salem sequences that were considered above. $\square$

Proof of Theorem 1.4. Suppose that the relation (1.1) holds with some $k_j \in \mathbb{Z}$, not all zero, and conjugates α_j of a Salem number α labelled as in Theorem 1.1. Then, by Theorem 1.1, we must have $k_{2j} = k_{2j-1}$ for $j = 1, \dots, s$. Setting $\beta_j = \alpha_{2j-1} + 1/\alpha_{2j-1}$ for $j = 1, \dots, s$ we find that (1.3) holds, namely, $k_1\beta_1 + k_3\beta_2 + \dots + k_{2s-1}\beta_s = 0$.

In order to prove the first part of the theorem we need to show that $|k_1| + |k_3| + \dots + |k_{2s-1}| \geq 3$. For a contradiction, assume that

$$|k_1| + |k_3| + \dots + |k_{2s-1}| \leq 2.$$

The case when $|k_{2j-1}| = 2$ for some j (and so other k_{2i-1} are all zeros) is clearly impossible, since $\pm 2\beta_j \neq 0$. Therefore, we must have $|k_{2i-1}| = |k_{2l-1}| = 1$, where $i < l$, and $k_{2j-1} = 0$ for each $j \neq i, l$. Dividing both sides of the relation $k_{2i-1}\beta_i + k_{2l-1}\beta_l = 0$ by k_{2i-1}, we find that $\beta_i = -k_{2l-1}\beta_l/k_{2i-1} = \pm\beta_l$. Since $\beta_i \neq \beta_l$, the only possibility is $\beta_i = -\beta_l$. Applying to it any automorphism σ that maps β_i to $\beta_1 > 2$ one obtains $\beta_1 = -\sigma(\beta_l)$. Here, the left hand side is a real number greater than 2, whereas the right hand side belongs to the interval $(-2, 2)$, which is a contradiction.

In order to prove the existence of a Salem number of degree 12 with required linear relation among its conjugates we can take, for instance, the following two pairs of real numbers (a, b):

$$(a_1, b_1) = (5-\sqrt{2}, -3+2\sqrt{2}) \quad \text{and} \quad (a_2, b_2) = (5+\sqrt{2}, -3-2\sqrt{2}).$$

Here, the first pair (a_1, b_1) satisfies $0 < a_1 < 4$ and (2.1), since $b_1 = -0.171572\dots$ and the left and right hand sides of (2.1) are $-0.828427\dots$ and $0.828427\dots$, respectively. Thus, by Lemma 2.1, $x^3 - a_1x + b_1$ has three roots in $(-2, 2)$.

The second pair (a_2, b_2) satisfies $3 < a_2 < 12$ and (2.2), because $b_2 = -5.828427\dots$ and the left and right hand sides of (2.2) are $-6.252637\dots$

and $-4.8284427\ldots$, respectively. Hence, by Lemma 2.1, $x^3 - a_2x + b_2$ has two roots in $(-2, 2)$ and one greater than 2.

Consequently, their product

$$\begin{aligned} g(x) :&= (x^3 - a_1x + b_1)(x^3 - a_2x + b_2) \\ &= (x^3 - 5x - 3 + \sqrt{2}(x+2))(x^3 - 5x - 3 - \sqrt{2}(x+2)) \\ &= x^6 - 10x^4 - 6x^3 + 23x^2 + 22x + 1 \end{aligned}$$

has 5 roots in $(-2, 2)$ and one greater than 2. Now,

$$f(x) := x^6 g(x + 1/x)$$

equals to

$$x^{12} - 4x^{10} - 6x^9 - 2x^8 + 4x^7 + 7x^6 + 4x^5 - 2x^4 - 6x^3 - 4x^2 + 1.$$

This polynomial defines a Salem number $\alpha = 2.502568\ldots$, since f is irreducible over $\mathbb{Q}$.

We remark than none of the choices with $\sqrt{2}$ replaced by $\sqrt{3}$ or $\sqrt{5}$ works. The pairs $(a_1, b_1) = (5 - \sqrt{3}, -3 + 2\sqrt{3})$ and $(a_2, b_2) = (5 + \sqrt{3}, -3 - 2\sqrt{3})$ satisfy the requirements of Lemma 2.1. However, the polynomial g (and so f) is reducible:

$$\begin{aligned} g(x) :&= (x^3 - 5x - 3 + \sqrt{3}(x+2))(x^3 - 5x - 3 - \sqrt{3}(x+2)) \\ &= x^6 - 10x^4 - 6x^3 + 22x^2 + 18x - 3 \\ &= (x^2 - 3)(x^4 - 7x^2 - 6x + 1). \end{aligned}$$

Similarly, with the pairs $(a_1, b_1) = (5 - \sqrt{5}, -3 + 2\sqrt{5})$ and $(a_2, b_2) = (5 + \sqrt{5}, -3 - 2\sqrt{5})$ one also obtains g with 5 roots in $(-2, 2)$ and one in $(2, +\infty)$, but g (and so f) is reducible:

$$\begin{aligned} g(x) :&= (x^3 - 5x - 3 + \sqrt{5}(x+2))(x^3 - 5x - 3 - \sqrt{5}(x+2)) \\ &= x^6 - 10x^4 - 6x^3 + 20x^2 + 10x - 11 \\ &= (x^2 + x - 1)(x^4 - x^3 - 8x^2 + x + 11). \end{aligned}$$

By Corollary 1.2, there no Salem numbers of degree 4 or 6 with a nontrivial linear relation among its conjugates. To give the example of a Salem number of degree 8 with nontrivial linear relation among its conjugates we can take, for instance, $h(x) := x^2 + 4x + 1$ with roots $\gamma_1 = -2 - \sqrt{3}$ and $\gamma_2 = -2 + \sqrt{3}$ satisfying the conditions of Lemma 2.3. Then,

$$\begin{aligned} f(x) :&= x^4 h((x + 1/x)(1 - x - 1/x)) \\ &= x^8 - 2x^7 + x^6 - 2x^5 + x^4 - 2x^3 + x^2 - 2x + 1 \end{aligned}$$

is irreducible. Hence, by Lemma 2.3, f defines a Salem number $\alpha = 1.994004\ldots$ of degree 8 whose conjugates satisfy (2.6) with $k = 2$.

As above, not every choice of an irreducible h produces the irreducible polynomial f. For example, selecting $h(x) := x^2 + 4x + 2$ whose roots $\gamma_1 = -2 - \sqrt{2}$ and $\gamma_2 = -2 + \sqrt{2}$ satisfy the conditions of Lemma 2.3, we get the polynomial

$$\begin{aligned} f(x) : &= x^4 h\big((x + 1/x)(1 - x - 1/x)\big) \\ &= x^8 - 2x^7 + x^6 - 2x^5 + 2x^4 - 2x^3 + x^2 - 2x + 1 \\ &= (x^4 + 1)(x^4 - 2x^3 + x^2 - 2x + 1), \end{aligned}$$

which is reducible. $\square$

References

[1] G. Baron, M. Drmota & M. Skałba, "Polynomial relations between polynomial roots", *J. Algebra* **177** (1995), p. 827-846.

[2] F. Beukers & C. J. Smyth, "Cyclotomic points on curves", in *Number theory for the millennium I. Proceedings of the millennial conference on number theory, Urbana-Champaign, IL, USA, May 21–26, 2000*, A K Peters, 2002, p. 21-26.

[3] D. W. Boyd, "Small Salem numbers", *Duke Math. J.* **44** (1977), p. 315-328.

[4] C. Christopoulos & J. McKee, "Galois theory of Salem polynomials", *Proc. Camb. Philos. Soc.* **148** (2010), no. 1, p. 47-54.

[5] J. D. Dixon, "Polynomials with nontrivial relations between their roots", *Acta Arith.* **82** (1997), no. 3, p. 293-302.

[6] M. Drmota & M. Skałba, "On multiplicative and linear independence of polynomial roots", in *Proceedings of the Vienna conference, June 14-17, 1990, Vienna, Austria*, Contributions to General Algebra, vol. 7, Hölder-Pichler-Tempsky; Teubner, 1991, p. 127-135.

[7] ———, "Relations between polynomial roots", *Acta Arith.* **71** (1995), no. 1, p. 65-77.

[8] A. Dubickas, "On the degree of a linear form in conjugates of an algebraic number", *Ill. J. Math.* **46** (2002), no. 2, p. 571-585.

[9] ———, "Additive relations with conjugate algebraic numbers", *Acta Arith.* **107** (2003), no. 1, p. 35-43.

[10] A. Dubickas, K. G. Hare & J. Jankauskas, "No two non-real conjugates of a Pisot number have the same imaginary part", *Math. Comput.* **86** (2017), no. 304, p. 935-950.

[11] A. Dubickas & J. Jankauskas, "Simple linear relations between conjugate algebraic numbers of low degree", *J. Ramanujan Math. Soc.* **30** (2015), no. 2, p. 219-235.

[12] A. Dubickas & C. J. Smyth, "On the lines passing through two conjugates of a Salem number", *Proc. Camb. Philos. Soc.* **144** (2008), no. 1, p. 29-37.

[13] M. Filaseta, K. Ford & S. Konyagin, "On an irreducibility theorem of A. Schinzel associated with coverings of the integers", *Ill. J. Math.* **44** (2000), no. 3, p. 633-643.

[14] M. Filaseta & M. j. Matthews, "On the irreducibility of 0, 1-polynomials of the form $f(x)x^n + g(x)$", *Colloq. Math.* **99** (2004), no. 1, p. 1-5.

[15] K. Girstmair, "Linear relations between roots of polynomials", *Acta Arith.* **89** (1999), no. 1, p. 53-96, corrigendum in *ibid.* **110** (2003), no. 2, p. 203.

[16] V. A. Kurbatov, "On equations of prime degree", *Mat. Sb., N. Ser.* **43** (1957), p. 349-366.

[17] ———, "Linear dependence of conjugate elements", *Mat. Sb., N. Ser.* **52** (1960), p. 701-708.

[18] ———, "Galois extensions of prime degree and their primitive elements", *Izv. Vyssh. Uchebn. Zaved., Mat.* **21** (1977), p. 49-52.

[19] F. Lalande, "La relation linéaire $a = b + c + \cdots + t$ entre les racines d'un polynôme", *J. Théor. Nombres Bordeaux* **19** (2007), no. 2, p. 473-484.

[20] ———, "À propos de la relation galoisienne $x_1 = x_2 + x_3$", *J. Théor. Nombres Bordeaux* **22** (2010), no. 3, p. 661-673.

[21] J. McKee & C. J. Smyth, "There are Salem numbers of every trace", *Bull. Lond. Math. Soc.* **37** (2005), no. 1, p. 25-36.

[22] R. Salem, "A Remarkable Class of Algebraic Numbers. Proof of a Conjecture of Vijayaraghavan", *Duke Math. J.* **11** (1944), p. 103-107.
[23] ———, "Power series with integral coefficients", *Duke Math. J.* **12** (1945), p. 153-173.
[24] A. Schinzel, "Reducibility of polynomials and covering systems of congruences", *Acta Arith.* **13** (1967), p. 91-101.
[25] C. J. Smyth, "Conjugate algebraic numbers on conics", *Acta Arith.* **40** (1982), p. 333-346.
[26] ———, "Additive and multiplicative relations connecting conjugate algebraic numbers", *J. Number Theory* **23** (1986), p. 243-254.
[27] ———, "Salem numbers of negative trace", *Math. Comput.* **69** (2000), no. 230, p. 827-838.
[28] A. Valibouze, "Sur les relations entre les racines d'un polynôme", *Acta Arith.* **131** (2008), no. 1, p. 1-27.

Artūras Dubickas
Institute of Mathematics
Faculty of Mathematics and Informatics
Vilnius University
Naugarduko 24
03225 Vilnius, Lithuania
E-mail: `arturas.dubickas@mif.vu.lt`
URL: `http://www.mif.vu.lt/~dubickas`

Jonas Jankauskas
Mathematik und Statistik
Montanuniversität Leoben
Franz Josef Strasse 18
8700 Leoben, Austria
E-mail: `jonas.jankauskas@gmail.com`
URL: `http://www.mif.vu.lt/~jonajank`