Elemente der Mathematik (Online first)
DOI 10.4171/EM/532

Published by EMS Press

Schanuel's conjecture and the roots of elementary functions

Miklós Laczkovich

Miklos Laczkovich graduated from the Eötvös Loránd University (Budapest). He is an emeritus professor of mathematics at Eötvös Loránd University and at University College London.

1 Introduction and main results

In the history of the negative solution of Hilbert's tenth problem, one of the major steps was made by Martin Davis, Hilary Putnam and Julia Robinson. They proved in [3] that there is a polynomial $P \in \mathbb{Z}[y, x_1, \dots, x_{2n}]$ such that the set of positive integers y for which the equation

$$P(y, x_1, \dots, x_n, 2^{x_1}, \dots, 2^{x_n}) = 0$$

is solvable in positive integers is not recursive. Let $\mathcal{E}$ denote the smallest class of real functions such that (i) $\mathcal{E}$ contains the constant functions 1, $\log 2$, π, the functions x, $\sin x$, e^x, and (ii) $\mathcal{E}$ is closed under addition, subtraction, multiplication and composition. Based on the Davis–Putnam–Robinson theorem, D. Richardson proved in [7] that it is recursively

Nach dem Satz von D. Richardson ist es rekursiv unentscheidbar, ob eine Elementarfunktion eine reelle Nullstelle hat oder nicht. Genauer gesagt gilt: Ist $\mathcal{E}$ die kleinste unter Addition, Subtraktion, Multiplikation und Komposition abgeschlossene Klasse von reellen Funktionen, welche die konstanten Funktionen 1, $\log 2$, π und die Funktionen x, $\sin x$, e^x enthält, dann ist es rekursiv unentscheidbar, ob ein gegebenes Element von $\mathcal{E}$ eine reelle Nulstelle hat oder nicht. Es gibt Unterklassen von $\mathcal{E}$ mit der gleichen Eigenschaft. Die kleinste bekannte solche Klasse ist der Ring $\mathcal{S}_1$ erzeugt durch die Funktionen 1, x, $\sin x^n$ und $\sin(x \cdot \sin x^n)$ $(n = 1, 2, \dots)$. Im vorliegenden Artikel wird gezeigt, dass die Funktionen $\sin(x \cdot \sin x^n)$ nicht aus $\mathcal{S}_1$ entfernt werden können, ohne diese Eigenschaft zu verlieren. Unter der Annahme, dass die Vermutung von Schanuel in der transzendenten Zahlentheorie richtig ist, wird ein Algorithmus angegeben, der für jedes Element f des von 1, x, $\sin x^n$ und $\cos x^n$ $(n = 1, 2, \dots)$ erzeugten Ringes entscheidet, ob f eine reelle Nullstelle in einem gegebenen Intervall hat. Dasselbe wird gemacht für den durch 1, $\sin x^n$ und $\cos x^n$ erzeugten Ring.

undecidable if an element of $\mathcal{E}$ has a real root or has a positive value. When Matiyasevich completed the solution of Hilbert's tenth problem in 1970, it became clear that the functions $\log 2$ and e^x can be removed from the class $\mathcal{E}$. Let $\mathcal{S}$ denote the smallest class of real functions which contains the constant functions 1, π, the functions x, $\sin x$, and which is closed under addition, subtraction, multiplication and composition. It was proved by P. S. Wang in [12] (based on the papers of D. Richardson and B. F. Caviness [1] as well) that it is recursively undecidable if an element of $\mathcal{S}$ has a real root or has a positive value.

The class $\mathcal{S}$ was further reduced in the paper [5], where it was shown that the existence of a zero or a positive value of a function is still recursively undecidable in the ring $\mathcal{S}_1$ generated by the identically 1 function and the functions x, $\sin x^n$ and $\sin(x \cdot \sin x^n)$ $(n = 1, 2, \ldots)$ defined on $\mathbb{R}$. That is, the constant function π can be removed from $\mathcal{S}$, and the number of compositions used to form the elements of $\mathcal{S}$ can be restricted. Now the class $\mathcal{S}_1$ is not very far from being optimal, that is, being smallest. Let $\mathcal{S}_2$ be the ring generated by the identically 1 function and the functions $\sin x^n$ and $\cos x^n$ $(n = 1, 2, \ldots)$. It was proved in [5] that there is an algorithm that decides if an element of $\mathcal{S}_2$ has a positive value. The problem whether or not there is an algorithm that decides if an element of $\mathcal{S}_2$ has a real root remained open.

The following simple example shows that such an algorithm, if it exists, must rely on some facts of number theory. Suppose we have to decide if the function $2 + \cos x + \cos x^2$ has a real root. Clearly, α is a real root if and only if $\cos\alpha = \cos\alpha^2 = -1$. Therefore, a real root exists if and only if there are integers k, n such that $((2k+1)\pi)^2 = (2n+1)\pi$, that is, if $\pi = (2n+1)/(2k+1)^2$. We know that no such integers exist, as π is irrational, so there is no real root. Conversely, the fact that there is no real root implies that π is irrational, or at least it is not a rational number with odd numerator and denominator.

Conjectures in number theory appear in several decision problems. Already Caviness used a number theoretic conjecture to solve the identity problem to a certain class of exponential expressions in [1]. The conjecture used most often in this context is *Schanuel's conjecture*, abbreviated as (SC). It states that *if $x_1, \ldots, x_n$ are $\mathbb{Q}$-linearly independent complex numbers, then the transcendence degree of the field $\mathbb{Q}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$ over $\mathbb{Q}$ is at least n*. (See [9,11].) Out of the several applications of (SC), we only mention here the decidability of the real exponential field proved by A. Macintyre and A. J. Wilkie (see [6,13]), A. C. Shkop's theorem on the algebraic roots of exponential polynomials [8], and the proof of Shapiro's conjecture by P. D'Aquino, A. Macintyre and G. Terzo [2].

In this note, we show that, assuming (SC), the existence of roots of the elements of $\mathcal{S}_2$ can be decided algorithmically.

Theorem 1.1. *Assuming* (SC)*, there is an algorithm that decides if an element of $\mathcal{S}_2$ has a real root or not.*

We also consider the larger ring $\mathcal{R}$ generated by the identically 1 function and the functions x, $\sin x^n$ and $\cos x^n$ $(n = 1, 2, \ldots)$ defined on $\mathbb{R}$. Unfortunately, in order to decide whether or not an element of $\mathcal{R}$ has a root or has a positive value, even (SC) does not seem to be strong enough. Suppose, e.g., that we want to decide whether or not the function $(x^2+1)\cdot(2+\cos x+\cos x^2) - 1$ has a negative value. We know that the function $2 + \cos x + \cos x^2$ takes arbitrarily small values, as the sequence of points $(\{\frac{k}{2\pi}\}, \{\frac{k^2}{2\pi}\})$ $(k = 1, 2, \ldots)$ is dense in $[0,1]^2$ (see the proof of Lemma 2.1 in the next section). But can

$2 + \cos x + \cos x^2$ be smaller than $1/(x^2 + 1)$? In order to answer questions of this type, we probably need very strong results on Diophantine approximations (see [10]).

Still, we can prove the following.

Theorem 1.2. *Suppose* (SC). *Then there is an algorithm that decides for every $f \in \mathcal{R}$ and for every subinterval I of $\mathbb{R}$ with rational endpoints whether or not f has a root in I.*

The proofs of Theorems 1.1 and 1.2 will be given in Section 4, using the results of the next two sections.

2 Representations of the elements of $\mathcal{R}$

The elements of the ring $\mathcal{R}$ are given in the form

$$f(x) = p(x, \sin x, \dots, \sin x^n, \cos x, \dots, \cos x^n), \tag{1}$$

where $p \in \mathbb{Q}[x, y_1, \dots, y_n, z_1, \dots, z_n]$. Replacing the powers $(\cos x^j)^{2k}$ by $(1 - \sin^2 x^j)^k$ in the right-hand side of (1) if necessary, we may assume that the polynomial p is such that the degree of each of the variables $z_1, \dots, z_n$ in p is at most 1. Polynomials with this property will be called *reduced*. Our first aim is to prove the following.

Lemma 2.1. *The representation of an element of $\mathcal{R}$ using a reduced polynomial is unique.*

We put

$$K_n = \{(y_1, \dots, y_n, z_1, \dots, z_n) \in \mathbb{R}^{2n} : y_j^2 + z_j^2 = 1 \ (j = 1, \dots, n)\}.$$

Lemma 2.2. *If a reduced polynomial $p \in \mathbb{Q}[y_1, \dots, y_n, z_1, \dots, z_n]$ vanishes on K_n, then $p = 0$.*

Proof. We prove the statement by induction. Suppose that either $n = 1$, or $n > 1$, and the statement is true for $n - 1$. We have

$$p = q + r \cdot z_n, \quad \text{where } q, r \in \mathbb{Q}[y_1, \dots, y_n, z_1, \dots, z_{n-1}].$$

Note that both q and r are reduced. Since p vanishes on K_n, we have $q = -r \cdot z_n$ and

$$q^2 = r^2 \cdot z_n^2 = r^2 \cdot (1 - y_n^2) \tag{2}$$

on K_n. If $n = 1$, then we obtain that $q^2 = r^2 \cdot (1 - y_1^2)$ holds on $[-1, 1]$; therefore, it holds everywhere on $\mathbb{R}$. If $q \neq 0$, then unique factorization in $\mathbb{Q}[y_1]$ implies that $(1 - y_1^2)$ is a (constant multiple of a) square in $\mathbb{Q}[y_1]$, which is not the case. Thus $q = 0$, $r = 0$ and $p = 0$.

Suppose that $n > 1$, and the statement is true for $n - 1$. Then (2) implies that

$$q^2 - r^2 \cdot (1 - y_n^2) = 0$$

on $K_{n-1} \times [-1, 1]$. Fixing $y_n \in [-1, 1]$ and applying the induction hypothesis, we find that $q^2 - r^2 \cdot (1 - y_n^2) = 0$ holds on $\mathbb{R}^{2n-2} \times [-1, 1]$; therefore, it holds everywhere on $\mathbb{R}^{2n-1}$.

If $q \neq 0$, then unique factorization in $\mathbb{Q}[y_1, \dots, y_n, z_1, \dots, z_{n-1}]$ implies that $(1 - y_n^2)$ is a (constant multiple of a) square in $\mathbb{Q}[y_1, \dots, y_n, z_1, \dots, z_{n-1}]$, which is not the case. Thus $q = 0$, $r = 0$ and $p = 0$. ∎

Proof of Lemma 2.1. We have to prove that if the function f in (1) is identically zero, where p is reduced, then $p = 0$. First we show this in the case when p does not depend on x. It is well known that the sequence

$$\left(\left\{\frac{k}{2\pi}\right\}, \left\{\frac{k^2}{2\pi}\right\}, \dots, \left\{\frac{k^n}{2\pi}\right\}\right) \quad (k = 1, 2, \dots)$$

is uniformly distributed in $[0, 1]^n$. (See [4, Theorem 6.3 on p. 48 and Theorem 3.2 on p. 27]). In particular, this sequence is everywhere dense in $[0, 1]^n$. Therefore, the set

$$\{(\sin k, \dots, \sin k^n, \cos k, \dots, \cos k^n) : k = 1, 2, \dots\} \tag{3}$$

is everywhere dense in K_n. Since f is identically zero, it follows that p vanishes on a dense subset of K_n; hence it vanishes on K_n. Then, by Lemma 2.2, $p = 0$.

Now we turn to the general case. If $p \neq 0$, then $p = x^m \cdot p_m + \dots + x \cdot p_1 + p_0$, where $p_j \in \mathbb{Q}[y_1, \dots, y_n, z_1, \dots, z_n]$ $(j = 0, \dots, m)$ and $p_m \neq 0$. Then we have $f(x) = x^m \cdot g_m + \dots + x \cdot g_1 + g_0$, where

$$g_j(x) = p_j(\sin x, \dots, \sin x^n, \cos x, \dots, \cos x^n) \quad (j = 0, \dots, m).$$

By Lemma 2.2, we have $p_m|_{K_n} \neq 0$. Let $x \in K_n$ be such that $c = p_m(x) \neq 0$. Since the set (3) is everywhere dense in K_n, we can find a sequence $k_\nu \to \infty$ such that

$$\lim_{\nu \to \infty} (\sin k_\nu, \dots, \sin k_\nu^n, \cos k_\nu, \dots, \cos k_\nu^n) = x$$

and $g_m(k_\nu) \to c$ as $\nu \to \infty$. Then $f(k_\nu) \cdot k_\nu^{-m} \to c$ as $\nu \to \infty$, which is impossible, as $f = 0$ by assumption. This proves $p = 0$. ∎

We also need a different representation of the elements of $\mathcal{R}$. Let $f \in \mathcal{R}$ be given by (1). Applying the identities

$$\sin x = \frac{2\tan(x/2)}{1 + \tan^2(x/2)}, \quad \cos x = \frac{1 - \tan^2(x/2)}{1 + \tan^2(x/2)},$$

we get

$$f(x) = r\big(x, \tan(x/2), \dots, \tan(x^n/2)\big),$$

where $r \in \mathbb{Q}(x_0, x_1, \dots, x_n)$, and the denominator of r is a product of factors of the form $1 + x_j^2$ $(j = 1, \dots, n)$. Since $1 + \tan^2(x^j/2) = 1/\cos^2(x^j/2)$, we obtain

$$f(x) = q\big(x, \tan(x/2), \dots, \tan(x^n/2)\big) \cdot \big(\cos(x/2)\big)^{a_1} \cdots \big(\cos(x^n/2)\big)^{a_n}, \tag{4}$$

where $q \in \mathbb{Q}[x_0, x_1, \dots, x_n]$ and $a_1, \dots, a_n$ are nonnegative even integers.

3 Lemmas on roots

Lemma 3.1. *There is an algorithm that decides for every $f \in \mathcal{R}$ whether or not f has a real root that is algebraic over $\mathbb{Q}$. There is also an algorithm that decides if $f \in \mathcal{R}$ has an algebraic root that belongs to a given subinterval of $\mathbb{R}$ with rational endpoints.*

Proof. Let f be given by (1), where $p \in \mathbb{Q}[x, y_1, \dots, y_n, z_1, \dots, z_n]$. Applying Euler's identities, we find $f = e^{i \cdot S} \cdot F$, where $S \in \mathbb{Z}[x]$ and F is a polynomial of $x, e^{ix}, \dots, e^{ix^n}$ with coefficients belonging to $\mathbb{Q}(i)$. Clearly, the roots of f and F coincide. We can write F in the form $\sum_{j=1}^{N} p_j \cdot e^{i \cdot s_j}$, where $p_j \in \mathbb{Q}(i)[x]$ and $s_j \in \mathbb{Z}[x]$ for every $j = 1, \dots, N$. We may assume that $s_1, \dots, s_N$ are different, and $p_j \neq 0$ for every $j = 1, \dots, N$.

Suppose that α is an algebraic root of f, and let g denote the minimal polynomial of α. Since it is clear how to decide whether or not 0 is a root of f, we may assume that $\alpha \neq 0$. Let d denote the degree of g; then $d \geq 1$.

Let $s_j = q_j \cdot g + r_j$, where $q_j, r_j \in \mathbb{Q}[x]$ and $\deg r_j < d$ for every $j = 1, \dots, N$. Then $s_j(\alpha) = s_k(\alpha)$ if and only if $r_j = r_k$. Rearranging the terms if necessary, we may assume that $r_1, \dots, r_m$ are distinct, and r_j equals one of $r_1, \dots, r_m$ for every $j = m+1, \dots, N$. Let P_j denote the sum of those polynomials p_k for which $r_k = r_j$. Then we have

$$\sum_{j=1}^{m} P_j(\alpha) \cdot e^{i \cdot r_j(\alpha)} = F(\alpha) = 0. \tag{5}$$

We prove that each of the numbers $P_j(\alpha)$ $(j = 1, \dots, m)$ must be zero.

From the fact that $\deg g = d$, it follows that the numbers $i, i\alpha, \dots, i\alpha^{d-1}$ are linearly independent over $\mathbb{Q}$. By the Lindemann–Weierstrass theorem, this implies that the numbers $e^{i}, \dots, e^{i\alpha^{d-1}}$ are algebraically independent over $\mathbb{Q}$.

Let D denote the common denominator of the coefficients of $r_1, \dots, r_m$, and put $u_t = e^{i\alpha^t/D}$ $(t = 0, \dots, d-1)$. Then $u_0, \dots, u_{d-1}$ are also algebraically independent over $\mathbb{Q}$. Each number $e^{i \cdot r_j(\alpha)}$ $(j = 1, \dots, m)$ is a product U_j of powers of $u_0, \dots, u_{d-1}$ with integer exponents. Since the values $r_1(\alpha), \dots, r_m(\alpha)$ are distinct, it follows that the products U_j are formally different. Since $u_0, \dots, u_{d-1}$ are algebraically independent over $\mathbb{Q}$, the numbers $P_j(\alpha)$ are algebraic, and $\sum_{j=1}^{m} P_j(\alpha) \cdot U_j = 0$ by (5), it follows that $P_j(\alpha) = 0$ for every $(j = 1, \dots, m)$, as we stated.

Since $P_j \in \mathbb{Q}(i)[x]$, it follows that $g \mid P_j \cdot \overline{P_j}$ in $\mathbb{Q}[x]$, where $\overline{P_j}$ is obtained from P_j by taking the complex conjugates of its coefficients. The previous considerations imply that if $g \in \mathbb{Q}[x]$ is an irreducible polynomial such that f vanishes at a real root of g, then f vanishes at each real root of g. We can also see that the number of these polynomials is finite. Indeed, the number of possibilities in forming the polynomials $P_1, \dots, P_m$ (by partitioning $p_1, \dots, p_N$ and taking the sum of each group) is finite. Take any of these systems $P_1, \dots, P_m$. If the polynomial P_1 is nonzero, then g is a divisor of $P_1 \cdot \overline{P_1}$. The number of possible polynomials g with this property is finite, and they can be found by factorizing all the possible polynomials $P_1 \cdot \overline{P_1}$.

Next suppose that P_1 is identically zero. Since $p_j \neq 0$ for every $j = 1, \dots, N$, and P_1 is the sum of those polynomials p_j for which $r_j = r_1$, there must be at least one $j > 1$ such that $r_j = r_1$. Then g divides $s_j - s_1$, which shows that the number of possible polynomials

g with this property is finite again, and they can be found by factorizing the polynomials $s_j - s_1$ $(1 < j \le N)$.

If $g \in \mathbb{Q}[x]$ is a given irreducible polynomial, then following the argument leading to equation (5), we can decide whether or not the real roots of g are roots of f as well. Then, using Sturm's algorithm, we can decide if g has a real root or has a root in a given interval. This completes the proof. ∎

The proof above shows that the nonzero elements of $\mathcal{R}$ only have finitely many algebraic roots. Under (SC), this is true for a much larger class; see [8].

Lemma 3.2. *Assume* (SC). *Suppose f is represented by* (1)*, where p is reduced, and let $1 \le j \le n$. Then f and $\cos(x^j/2)$ have a common real root if and only if, substituting $y_j = 0$ and $z_j = -1$ into p, it becomes identically zero.*

Proof. If $\cos(\alpha^j/2) = 0$, then $\sin\alpha^j = 0$ and $\cos\alpha^j = -1$. It is clear that if the substitution $y_j = 0, z_j = -1$ makes p zero, then $f(\alpha) = 0$. This proves the "if" statement of the lemma.

Now suppose that f and $\cos(x^j/2)$ have a common real root α. In order to make the notation simpler, we assume that $j = n$. (The proof is the same in the other cases.) Put

$$p_1(x, y_1, \dots, y_{n-1}, z_1, \dots, z_{n-1}) = p(x, y_1, \dots, y_{n-1}, 0, z_1, \dots, z_{n-1}, -1).$$

Note that p_1 is reduced. Since $f(\alpha) = 0$, we have $g(\alpha) = 0$, where

$$g(x) = p_1(x, \sin x, \dots, \sin x^{n-1}, \cos x, \dots, \cos x^{n-1}).$$

In order to prove that $p_1 = 0$, it is enough to show, by Lemma 2.1, that g is identically zero. Using Euler's identities, we can find polynomials

$$S \in \mathbb{Z}[x] \quad \text{and} \quad p_2 \in \mathbb{Q}(i)[x_0, x_1, \dots, x_{n-1}]$$

such that $g(x) = e^{iS(x)} \cdot p_2(x, e^{ix}, \dots, e^{ix^{n-1}})$. Therefore, we have

$$p_2(\alpha, e^{i\alpha}, \dots, e^{i\alpha^{n-1}}) = 0. \tag{6}$$

Since $\cos(\alpha^n/2) = 0$, we have $e^{i\alpha^n} = -1$, and then it follows from Lindemann's theorem that α is transcendental. Then $\alpha, \alpha^2, \dots, \alpha^n$ are linearly independent over $\mathbb{Q}$. By (SC), the transcendence degree of the field $\mathbb{Q}(i\alpha, \dots, i\alpha^n, e^{i\alpha}, \dots, e^{i\alpha^n})$ is at least n. Since $e^{i\alpha^n} = -1$, we obtain that the numbers $\alpha, e^{i\alpha}, \dots, e^{i\alpha^{n-1}}$ are algebraically independent over $\mathbb{Q}$. Therefore, by (6), we have $p_2 = 0$, and thus g is identically zero. ∎

Let $q \in \mathbb{Q}[x_0, x_1, \dots, x_n]$, $q \ne 0$, and let d_j denote the degree of x_j in q. It is clear that

$$q\big(x, \tan(x/2), \dots, \tan(x^n/2)\big) \cdot \big(\cos(x/2)\big)^{d_1} \cdots \big(\cos(x^n/2)\big)^{d_n} \tag{7}$$

is a polynomial of the functions x, $\sin(x^j/2)$ and $\cos(x^j/2)$ $(j = 1, \dots, n)$, and thus it is defined everywhere on $\mathbb{R}$. Let f denote this function.

Lemma 3.3. *Suppose* (SC). *Then f does not vanish at the roots of $\cos(x^j/2)$ for every $j = 1, \dots, n$.*

Proof. We only prove the statement for $j = n$; the proof of the other cases is the same. We have

$$q = \sum_{j=0}^{d_n} x_n^j \cdot q_j,$$

where $q_j \in \mathbb{Q}[x_0, x_1, \dots, x_{n-1}]$ for every $j = 0, \dots, d_n$ and $q_{d_n} \neq 0$. Put $h_j(x) = q_j(x, \tan(x/2), \dots, \tan(x^{n-1}/2))$ and

$$f_j(x) = h_j(x) \cdot \big(\cos(x/2)\big)^{d_1} \cdots \big(\cos(x^{n-1}/2)\big)^{d_{n-1}}.$$

Then

$$f(x) = \sum_{j=0}^{d_n} \big(\sin(x^n/2)\big)^j \cdot \big(\cos(x^n/2)\big)^{d_n - j} \cdot f_j(x).$$

If $\cos(\alpha^n/2) = 0$, then $\sin(\alpha^n/2) = \pm 1$, and we have $f(\alpha) = \pm f_{d_n}(\alpha)$. We show that $f_{d_n}(\alpha) \neq 0$.

Since $\cos(\alpha^n/2) = 0$, we have $e^{i\alpha^n} = -1$, and it follows from Lindemann's theorem that α is transcendental. As we saw in the proof of Lemma 3.2, (SC) implies that $\alpha, e^{i\alpha}, \dots, e^{i\alpha^{n-1}}$ are algebraically independent over $\mathbb{Q}$. Thus $\cos(\alpha^j/2)$ is transcendental, hence nonzero for every $1 \leq j \leq n-1$. Since

$$h_{d_n}(\alpha) = q_{d_n}\big(\alpha, \tan(\alpha/2), \dots, \tan(\alpha^{n-1}/2)\big)$$

and $q_{d_n} \neq 0$, it follows that $h_{d_n}(\alpha)$ is nonzero. Then $f_{d_n}(\alpha)$ is nonzero as well. ∎

We put $A_n = \{x \in \mathbb{C} : x \text{ is algebraic over } \mathbb{Q} \text{ of degree less than } n\}$.

Lemma 3.4. *Assume* (SC). *Let* $p, q \in \mathbb{Q}[x_0, x_1, \dots, x_n]$, *and suppose that the functions*

$$f(x) = p\big(x, \tan(x/2), \dots, \tan(x^n/2)\big) \quad \textit{and} \quad g(x) = q\big(x, \tan(x/2), \dots, \tan(x^n/2)\big)$$

have a common root $\alpha \notin A_n$ *such that* $\cos(\alpha^j/2) \neq 0$ *for every* $j = 1, \dots, n$. *If* p *is irreducible in* $\mathbb{Q}[x_0, x_1, \dots, x_n]$, *then* $p \mid q$.

Proof. We put $t_0 = \alpha$ and $t_j = \tan(\alpha^j/2)$ for every $j = 1, \dots, n$. Since $\alpha \notin A_n$, the numbers $i\alpha, \dots, i\alpha^n$ are $\mathbb{Q}$-linearly independent. Therefore, by (SC), the transcendence degree of the field $\mathbb{Q}(\alpha, e^{i\alpha}, \dots, e^{i\alpha^n})$ is at least n. Then the same is true for the field $\mathbb{Q}(\alpha, \tan(\alpha/2), \dots, \tan(\alpha^n/2)) = \mathbb{Q}(t_0, \dots, t_n)$. This means that there is an $0 \leq m \leq n$ such that the numbers t_j $(0 \leq j \leq n,\ j \neq m)$ are algebraically independent over $\mathbb{Q}$.

Let R denote the polynomial ring $\mathbb{Q}[\{x_0, x_1, \dots, x_n\} \setminus \{x_m\}]$, and write p and q as elements of the polynomial ring $R[x_m]$. Let K denote the quotient field of R. Then there are polynomials $a, b, d \in K[x_m]$ such that $ap + bq = d$, $d \neq 0$, and $d \mid p$, $d \mid q$ in $K[x_m]$.

Multiplying d by a suitable nonzero element of K, we may assume that $d \in R[x_m]$ and that d is primitive, that is, every common divisor (in R) of the coefficients of d is a nonzero rational number. Let r be a common denominator of the coefficients of a and b. Then r is a nonzero element of R, and

$$(ar) \cdot p + (br) \cdot q = dr. \tag{8}$$

Here ar, br, p, q, d are elements of $R[x_m]$, that is, of $\mathbb{Q}[x_0, \dots, x_n]$, and r is a nonzero element of R. Replacing x_j by t_j $(j = 0, \dots, n)$, the left-hand side of (8) becomes zero. Then $\overline{d} \cdot \overline{r} = 0$, where $\overline{d}$ and $\overline{r}$ are the values of d and r under the substitution. Since the elements t_j $(j \neq m)$ are algebraically independent over $\mathbb{Q}$, we have $\overline{r} \neq 0$. Therefore, we have $\overline{d} = 0$. This implies that d is not constant.

By $d \mid p$ in $K[x_m]$, we have $p = e \cdot d$, where $e \in K[x_m]$. Since d is primitive, it follows from Gauss' lemma and from the fact that unique factorization holds in R that $e \in R[x_m]$, and $d \mid p$ in $\mathbb{Q}[x_0, \dots, x_n]$. Similarly, we have $d \mid q$ in $\mathbb{Q}[x_0, \dots, x_n]$. Since p is irreducible and d is not constant, we have $e \in \mathbb{Q}$, $e \neq 0$, and thus $p \mid d \mid q$. ∎

Lemma 3.5. *Assume* (SC). *Let $q \in \mathbb{Q}[x_0, \dots, x_n]$ be an irreducible polynomial, and put $h(x) = q(x, \tan(x/2), \dots, \tan(x^n/2))$. Suppose $\alpha \notin A_n$ is a real root of h such that $\cos(\alpha^j/2) \neq 0$ for every $j = 1, \dots, n$. Then α is a simple root of h.*

Proof. Note that h is not identically zero by Lemma 3.3. Suppose that α is a root of multiplicity at least 2. Then α is also a root of h'. Now we have

$$\begin{aligned} h'(x) &= \frac{\partial q}{\partial x_0}\big(x, \tan(x/2), \dots, \tan(x^n/2)\big) \\ &\quad + \sum_{j=1}^{n} \frac{\partial q}{\partial x_j}\big(x, \tan(x/2), \dots, \tan(x^n/2)\big) \cdot (jx^{j-1}/2) \cdot \cos^{-2}(x^j/2) \\ &= s\big(x, \tan(x/2), \dots, \tan(x^n/2)\big), \end{aligned}$$

where

$$s = \frac{\partial q}{\partial x_0}(x_0, \dots, x_n) + \sum_{j=1}^{n} \frac{\partial q}{\partial x_j}(x_0, \dots, x_n) \cdot (jx_0^{j-1}/2) \cdot (1 + x_j^2) \in \mathbb{Q}[x_0, \dots, x_n].$$

Since q is irreducible, it follows from Lemma 3.4 that $q \mid s$. Let $s = r \cdot q$, where $r \in \mathbb{Q}[x_0, \dots, x_n]$. Thus

$$h'(x) = r\big(x, \tan(x/2), \dots, \tan(x^n/2)\big) \cdot h(x) \tag{9}$$

for every x such that $\cos(x^j/2) \neq 0$ $(j = 1, \dots, n)$. Now (9) implies that the multiplicity of α as a root of h' is at least the multiplicity of α as a root of h, which is clearly impossible, since h is analytic in a neighbourhood of α. Therefore, α must be a simple root of h. ∎

4 Proof of Theorems 1.1 and 1.2

Recall that $\mathcal{S}_2$ is the ring generated by the identically 1 function and the functions $\sin(x^n)$ and $\cos(x^n)$ $(n = 1, 2, \dots)$.

Lemma 4.1. *Assume* (SC). *Then there is an algorithm that decides, for every irreducible polynomial $q \in \mathbb{Q}[x_1, \dots, x_n]$ whether or not the function*

$$h(x) = q\big(\tan(x/2), \dots, \tan(x^n/2)\big)$$

has a real root.

Proof. Let $f(x) = h(x) \cdot (\cos(x/2))^{d_1} \cdots (\cos(x^n/2))^{d_n}$, where d_j denotes the degree of x_j in q for every $j = 1, \ldots, n$. By Lemma 3.3, f does not vanish at the roots of $\cos(x^j/2)$ for $j = 1, \ldots, n$. Therefore, the roots of f and h coincide, so it is enough to decide whether or not the function f has a real root.

It is clear that $f(2x) \in \mathcal{S}_2$. By [5, Theorem 2], there is an algorithm that decides whether or not $f(2x)$ has a positive value. Evidently, we can also decide if $f(2x)$ has a negative value. If $f(2x)$ has both positive and negative values, then f has a real root, and we are done.

Suppose we found that f does not have negative values, that is, $f \geq 0$ everywhere. Then, applying Lemma 3.1, we check if f has a real algebraic root. If there is one, we stop. If there is no such root, then f and, consequently, h only have transcendental real roots. Then it follows from Lemma 3.5 that every real root of h is simple.

Let α be such a root. Then it follows that h changes sign in a neighbourhood of α. Now we have $f = h \cdot g$, where $g(\alpha) \neq 0$. Then f also changes sign in a neighbourhood of α, which contradicts $f \geq 0$. This proves that, in this case, h does not have a real root. We proceed similarly if $f \leq 0$ everywhere. ∎

Now we turn to the *proof of Theorem* 1.1. Let $f \in \mathcal{S}_2$ be given. First we check, using Lemma 3.2, if f has common roots with $\cos(x^j/2)$ $(1 \leq j \leq n)$. If it has, then we are done. Otherwise, we find q and representation (4). Then f has a real root if and only if $h(x) = q(x, \tan(x/2), \ldots, \tan(x^n/2))$ has one.

We write q as the product of the irreducible polynomials $q_j \in \mathbb{Q}[x_1, \ldots, x_n]$, where $j = 1, \ldots, k$. For each j, we check, using Lemma 4.1, whether or not the function

$$h_j(x) = q_j\big(x, \tan(x/2), \ldots, \tan(x^n/2)\big)$$

has a real root. If any of them has one, then $h = h_1 \cdots h_k$ and f also have such a root; otherwise, neither h nor f has one. ∎

Lemma 4.2. *Assume* (SC). *Then there is an algorithm that decides, for every irreducible polynomial* $q \in \mathbb{Q}[x_0, x_1, \ldots, x_n]$ *whether or not the function*

$$h(x) = q\big(x, \tan(x/2), \ldots, \tan(x^n/2)\big)$$

has a real root in a given interval $[a, b]$ *with rational endpoints.*

Proof. Let f be the function in (7), where d_j denotes the degree of x_j in q $(j = 1, \ldots, n)$. By Lemma 3.3, the real roots of f and h coincide. Clearly, $f(2x) \in \mathcal{R}$.

Applying Lemma 3.1, we check if $f(2x)$ has a algebraic root in the interval $[2a, 2b]$. If there is one, we stop. If there is no such root, then f and, consequently, h only have transcendental roots in $[a, b]$. Then it follows from Lemma 3.5 that every root of h in $[a, b]$ is simple.

As we saw in the proof of Lemma 4.1, if h has a simple root in (a, b), then f changes sign in a neighbourhood of the root. Therefore, we only have three cases: (i) $f > 0$ in $[a, b]$, (ii) $f < 0$ in $[a, b]$, (iii) f takes both positive and negative values in $[a, b]$. We have to decide which one of these cases is true.

For every rational number r, we can compute $f(r)$ with an error smaller than any given positive number. Indeed, this follows from the fact that we can compute the terms of the Taylor series of $\cos x$ and $\sin x$, and can estimate the Lagrange remainders. Let $r_1, r_2, \dots$ be an enumeration of the rational numbers in $[a, b]$ listing every such number infinitely many times. Compute $f(r_n)$ with an error less than $1/n$ for every $n = 1, 2, \dots$. If f takes both positive and negative values in $[a, b]$, then this procedure will prove this in a finite number of steps.

If $f > 0$ in $[a, b]$, then this fact can also be proved in a finite number of steps. Indeed, if f is represented as in (1), then we can easily find an integer K such that $|f'| < K$ in $[a, b]$. Then we check for every $n = 1, 2, \dots$ if $f(a) > K/n$, $f(b) > K/n$ and $f(k/n) > K/n$ is true for every integer k with $a \le k/n \le b$. Suppose we find such an n. Then, for every $x \in [a, b]$, there is a point $c \in [a, b]$ such that $|x - c| \le 1/n$ and $f(c) > K/n$, and thus

$$f(x) \ge f(c) - |f(x) - f(c)| > \frac{K}{n} - K \cdot |x - c| > \frac{K}{n} - \frac{K}{n} = 0.$$

On the other hand, if $f > 0$ in $[a, b]$, then $f > \delta$ in $[a, b]$ with a suitable $\delta > 0$. In this case, if $n > K/\delta$, then $f(a) > K/n$, $f(b) > K/n$ and $f(k/n) > K/n$ will be true for every integer k with $a \le k/n \le b$. This shows that the procedure above proves that $f > 0$ in $[a, b]$ in a finite number of steps.

A similar procedure can prove that $f < 0$ in $[a, b]$, if this is the case. Therefore, running these three procedures simultaneously, we can decide in a finite number of steps which one of the cases (i), (ii), (iii) is true. ∎

Now Theorem 1.2 follows from Lemma 4.2 the same way as Theorem 1.1 is deduced from Lemma 4.1. ∎

Funding. The author was supported by the Hungarian National Foundation for Scientific Research, Grant No. K146922.

References

[1] B. F. Caviness, On canonical forms and simplification. *J. Assoc. Comput. Mach.* **17** (1970), 385–396 Zbl 0193.31302 MR 281386

[2] P. D'Aquino, A. Macintyre, and G. Terzo, From Schanuel's conjecture to Shapiro's conjecture. *Comment. Math. Helv.* **89** (2014), no. 3, 597–616 MR 3260843

[3] M. Davis, H. Putnam, and J. Robinson, The decision problem for exponential diophantine equations. *Ann. of Math. (2)* **74** (1961), 425–436 Zbl 0111.01003 MR 133227

[4] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*. Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York–London–Sydney, 1974 Zbl 0281.10001 MR 419394

[5] M. Laczkovich, The removal of π from some undecidable problems involving elementary functions. *Proc. Amer. Math. Soc.* **131** (2003), no. 7, 2235–2240 Zbl 1016.03008 MR 1963772

[6] A. Macintyre and A. J. Wilkie, On the decidability of the real exponential field. In *Kreiseliana*, pp. 441–467, A K Peters, Wellesley, MA, 1996 Zbl 0896.03012 MR 1435773

[7] D. Richardson, Some undecidable problems involving elementary functions of a real variable. *J. Symbolic Logic* **33** (1968), 514–520 Zbl 0175.27404 MR 239976

[8] A. C. Shkop, Schanuel's conjecture and algebraic roots of exponential polynomials. *Comm. Algebra* **39** (2011), no. 10, 3813–3823 Zbl 1257.03061 MR 2845603

[9] M. Waldschmidt, Open Diophantine problems. *Mosc. Math. J.* **4** (2004), no. 1, 245–305, 312 Zbl 1101.16032 MR 2074991

[10] M. Waldschmidt, Recent advances in Diophantine approximation. In *Number theory, analysis and geometry*, pp. 659–704, Springer, New York, 2012 Zbl 1271.11070 MR 2867937

[11] M. Waldschmidt, Schanuel's conjecture: algebraic independence of transcendental numbers. In *Colloquium De Giorgi 2013 and 2014*, pp. 129–137, Colloquia 5, Ed. Norm., Pisa, 2014 Zbl 1387.11057 MR 3379182

[12] P. S. Wang, The undecidability of the existence of zeros of real elementary functions. *J. Assoc. Comput. Mach.* **21** (1974), 586–589 Zbl 0289.68017 MR 363862

[13] A. J. Wilkie, Schanuel's conjecture and the decidability of the real exponential field. In *Algebraic model theory (Toronto, ON, 1996)*, pp. 223–230, NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci. 496, Kluwer Acad. Publ., Dordrecht, 1997 Zbl 0888.03022 MR 1481447

Miklós Laczkovich
Department of Analysis
Eötvös Loránd University
1117 Budapest, Hungary
miklos.laczkovich@gmail.com