On the Skolem Problem for Continuous Linear Dynamical Systems

Ventsislav Chonev, Joël Ouaknine, James Worrell

Oxford University

Abstract. The Continuous Skolem Problem asks whether a real-valued function satisfying an ordinary linear differential equation has a zero in a given interval of real numbers. This is a fundamental reachability problem arising in the analysis of continuous linear dynamical systems, including linear hybrid automata and continuous-time Markov chains. Not only is decidability of this problem open, but decidability is open even for the sub-problem in which a zero is sought in a bounded interval. In this paper we show decidability of the bounded problem subject to Schanuel's conjecture, a central conjecture in transcendental number theory. Regarding the unbounded case, by way of hardness we show that decidability of the Continuous Skolem Problem would entail a major new effectiveness result in Diophantine approximation, namely computability of the Diophantine-approximation types of all real algebraic numbers.

1 Introduction

The Continuous Skolem Problem is a fundamental decision problem concerning reachability in continuous-time linear dynamical systems. The problem asks whether a real-valued function satisfying an ordinary linear differential equation has a zero in a given interval of real numbers. More precisely, an instance of the problem comprises an interval $I \subseteq \mathbb{R}_{\geq 0}$ with rational endpoints and an ordinary differential equation

$$f^{(n)} + a_{n-1} f^{(n-1)} + \ldots + a_0 f = 0 \tag{1}$$

with the coefficients $a_0, \ldots, a_{n-1}$ and initial conditions $f(0), \ldots, f^{(n-1)}(0)$ being real algebraic numbers. Writing $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ for the unique solution of the differential equation that satisfies the initial conditions, the question is whether there exists $t \in I$ such that $f(t) = 0$. Decidability of this problem is currently open. Decidability of the sub-problem in which the interval I is bounded, called the Bounded Continuous Skolem Problem, is also open [2, Open Problem 17].

The nomenclature *Continuous Skolem Problem* is based on viewing the problem as a continuous analog of the Skolem Problem for linear recurrence sequences, which asks whether a given linear recurrence sequence has a zero term [11]. Whether the latter problem is decidable is an outstanding question in number theory and theoretical computer science; see, e.g., the exposition of Tao [19, Section 3.9].

The continuous dynamics of linear hybrid automata and the evolution of continuous-time Markov chains, amongst many other examples, are determined by linear differential equations of the form $\boldsymbol{x}'(t) = A\boldsymbol{x}(t)$, where $\boldsymbol{x}(t) \in \mathbb{R}^n$ and A is an $n \times n$ matrix of real numbers [1]. A basic reachability question in this context is whether, starting from an initial state $\boldsymbol{x}(0)$, the system reaches a target halfplane $\{\boldsymbol{y} \in \mathbb{R}^n : \boldsymbol{u}^T\boldsymbol{y} = 0\}$, where $\boldsymbol{u} \in \mathbb{R}^n$. For example, one can ask whether the continuous flow of a hybrid automaton in a given location leads to a particular transition guard being satisfied. Now the function $f(t) = \boldsymbol{u}^T\boldsymbol{x}(t)$ satisfies a linear differential equation of the form (1), so such reachability questions can immediately be reduced to the Continuous Skolem Problem (see [2] for further details). Moreover, under this reduction, time-bounded reachability problems map to instances of the Bounded Continuous Skolem Problem.

The *characteristic polynomial* of the linear differential equation (1) is

$$\chi(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_0\,.$$

Let $\lambda_1, \ldots, \lambda_m$ be the distinct roots of χ. Any solution of (1) has the form $f(t) = \sum_{i=1}^m P_i(t)e^{\lambda_i t}$, where the P_i are polynomials with algebraic coefficients that are determined by (and computable from) the initial conditions of the differential equation, see [2]. We call a function f in this form an *exponential polynomial.* The Continuous Skolem Problem can equivalently be formulated in terms of whether an exponential polynomial has a zero in a given interval of reals.

In this paper we show decidability of the Bounded Continuous Skolem Problem subject to Schanuel's Conjecture, a unifying conjecture in transcendental number theory, generalising both the Lindemann-Weierstrass Theorem and Baker's Theorem on linear independence of logarithms of algebraic numbers. A celebrated paper of MacIntyre and Wilkie [15] obtains decidability of the first-order theory of the real exponential field, assuming Schanuel's conjecture. While this result is relevant to the present paper, we emphasize that we are concerned here with complex exponentiation. Schanuel's conjecture is also invoked in the analysis of exponential polynomials in [8,20], although not in the context of decidability.

Intuitively, decidability of the Bounded Continuous Skolem Problem is non-trivial because an exponential polynomial f can approach 0 tangentially. It is not obvious *a priori* how to confirm the existence of a tangential zero by finite-precision numerical computation. Moreover it is clear that tangential zeros can arise: a very simple example is the exponential polynomial $f(t) = 2 + 2\cos(t)$. Note that in this case f can be written as a product of exponential polynomials $f(t) = (1 + e^{it})(1 + e^{-it})$, with the two factors having common zeros. More generally, assuming Schanuel's Conjecture, we show that any exponential polynomial admits a factorisation such that the zeros of each factor can be detected using finite-precision numerical computations. Our method however does not enable us to bound the precision required to find zeros, so, as yet, we have no complexity upper bound for our procedure.

In the unbounded case, by way of hardness, we show that decidability of the Continuous Skolem Problem would entail major new effectiveness results in Diophantine approximation. These results concern the behaviour of continued-fraction expansions of real algebraic numbers. As we discuss further in Section 4, currently almost nothing is known about such expansions for numbers of degree three or higher.

1.1 Related Work

As we have noted, the Continuous Skolem Problem can be seen as asking whether the solution of a differential equation $\boldsymbol{x}'(t) = A\boldsymbol{x}(t)$ reaches a target halfplane starting from initial position $\boldsymbol{x}(0)$. The corresponding problem of reaching a given target *vector* has recently been shown to be decidable in polynomial time [4,10].

The paper [2] gives some partial decidability results for the Continuous Skolem Problem. These results all require strong assumptions on the matrix A in the equation $\boldsymbol{x}'(t) = A\boldsymbol{x}(t)$, e.g., that A be a Metzler matrix or that A have dimension 2. Under similarly restrictive spectral assumptions on A [2, Theorem 14] shows how to reduce the Continuous Skolem Problem to the bounded problem. The reachability problem for linear flows $\boldsymbol{x}'(t) = A\boldsymbol{x}(t)$ has also been considered under the framework of o-minimal hybrid systems [13, Corollary 3.10]. Here again one requires strong spectral assumptions on A to obtain decidability, i.e., that A be nilpotent or that its spectrum be either entirely real or entirely imaginary.

For linear recurrence sequences, a relation is observed in [16] between Diophantine approximation properties of logarithms of algebraic numbers and the *Positivity Problem*: decide whether all terms of a given sequence are positive. However no such connection is known for the (discrete) Skolem Problem.

2 Mathematical Background

2.1 Zero Finding

Our procedure for computing zeros of exponential polynomials is based on a straightforward sampling method. Let $f : (a, b) \to \mathbb{R}$ be a differentiable function defined on a bounded open interval of reals with rational endpoints. Assume that given a rational argument $t \in (a, b)$ and positive error bound $\varepsilon \in \mathbb{Q}$ we can compute $f(t)$ to within additive error ε, i.e., we can compute $q \in \mathbb{Q}$ such that $|f(t) - q| < \varepsilon$. Assume also that we are given a bound M such that $|f'(t)| \leq M$ for all $t \in (a, b)$. Finally we suppose that the equations $f(t) = f'(t) = 0$ have no solution $t \in (a, b)$, i.e., f has no tangential zeros. Under the above assumptions we describe a procedure for computing zeros of f.

For each integer $N \geq 2$ we consider $N - 1$ evenly spaced sample points $s_j := \frac{(N-j)a+jb}{N}$, $j = 1, \ldots, N - 1$, in the interval (a, b). For each sample point s_j, we compute a rational number q_j such that $|q_j - f(s_j)| < \frac{1}{N}$ and proceed as follows:

1. If $q_{j_1} \geq \frac{1}{N}$ and $q_{j_2} \leq -\frac{1}{N}$ for some $j_1, j_2 \in \{1, \ldots, N - 1\}$ then output that f has a zero in (a, b).
2. If $q_j > \frac{M+1}{N}$ for all $k \in \{1, \ldots, N - 1\}$ or $q_j < -\frac{M+1}{N}$ for all $j \in \{1, \ldots, N - 1\}$ then output that f has no zero in (a, b).
3. If neither of the above hold then the result is inconclusive and we proceed to the next value of N.

It is not hard to see that the above procedure eventually terminates given our assumption that f has no tangential zeros in (a, b).

2.2 Number-Theoretic Algorithms

Recall that a standard way to represent an algebraic number α is by its minimal polynomial M and a numerical approximation of sufficient accuracy to distinguish α from the other roots of M [5, Section 4.2.1]. Given two algebraic numbers α and β under this representation, the *Field Membership Problem* is to determine whether $\beta \in \mathbb{Q}(\alpha)$ and, if so, to return a polynomial P with rational coefficients such that $\beta = P(\alpha)$. This problem can be decided using the LLL algorithm, see [5, Section 4.5.4].

Given the characteristic polynomial χ of a linear differential equation we can compute approximations to each of its roots $\lambda_1, \ldots, \lambda_m$ to within an arbitrarily small additive error [17]. Moreover, by repeatedly using an algorithm for the Field Membership Problem we can compute a primitive element θ for the splitting field of χ and representations of $\lambda_1, \ldots, \lambda_m$ as polynomials in θ. Thereby we can determine maximal $\mathbb{Q}$-linearly independent subsets of $\{\Re(\lambda_j) : 1 \leq j \leq m\}$ and $\{\Im(\lambda_j) : 1 \leq j \leq m\}$.

Let log denote the branch of the complex logarithm defined by $\log(re^{i\theta}) = \log(r) + i\theta$ for a positive real number r and $0 \leq \theta < 2\pi$. Recall that one can compute $\log z$ and e^z to within arbitrarily small additive error given a sufficiently precise approximation of z [3].

2.3 Laurent Polynomials

Fix non-negative integers r and s, and consider a single variable x and tuples of variables $\boldsymbol{y} = \langle y_1, \ldots, y_r \rangle$ and $\boldsymbol{z} = \langle z_1, \ldots, z_s \rangle$. Consider the ring of Laurent polynomials

$$\mathcal{R} := \mathbb{C}[x, y_1, y_1^{-1}, \ldots, y_r, y_r^{-1}, z_1, z_1^{-1}, \ldots, z_s, z_s^{-1}] ,$$

which can be seen as a localisation of the polynomial ring $\mathcal{A} := \mathbb{C}[x, y_1, \ldots, y_r, z_1, \ldots, z_s]$ in the multiplicative set generated by the set of variables $\{y_1, \ldots, y_r\} \cup \{z_1, \ldots, z_s\}$. The multiplicative units of $\mathcal{R}$ are the non-zero monomials in variables $y_1, \ldots, y_r$ and $z_1, \ldots, z_s$. As the localisation of a unique factorisation domain, $\mathcal{R}$ is itself a unique factorisation domain [6, Theorem 10.3.7]. From the proof of this fact it moreover easily follows that $\mathcal{R}$ inherits from $\mathcal{A}$ the properties that a polynomial with algebraic coefficients factors as a product of polynomials that also have algebraic coefficients and that this factorisation can be effectively computed [12].

We extend the operation of complex conjugation to a ring automorphism of $\mathcal{R}$ as follows. Given a polynomial

$$P = \sum_{j=1}^{n} a_j x^{u_j} {y_1}^{v_{j1}} \ldots {y_r}^{v_{jr}} {z_1}^{w_{j1}} \ldots {z_s}^{w_{js}} ,$$

where $a_1, \ldots, a_n \in \mathbb{C}$, define its conjugate to be

$$\overline{P} := \sum_{j=1}^{n} \overline{a_j} x^{u_j} {y_1}^{v_{j1}} \ldots {y_r}^{v_{jr}} {z_1}^{-w_{j1}} \ldots {z_s}^{-w_{js}} .$$

This definition corresponds to the intuition that variables x and $y_1, \ldots, y_r$ are real-valued, while variables $z_1, \ldots, z_s$ take values in the unit circle in the complex plane.

We will need the following proposition concerning polynomials in $\mathcal{R}$ that are associated with their conjugates. Here we use pointwise notation for exponentiation: given a tuple of integers $\boldsymbol{u} = \langle u_1, \ldots, u_s \rangle$, we write $\boldsymbol{z}^{\boldsymbol{u}}$ for the monomial $z_1^{u_1} \ldots z_s^{u_s}$.

Proposition 1. *Let $P \in \mathcal{R}$ be such that $P = \boldsymbol{z}^{\boldsymbol{u}}\overline{P}$ for $\boldsymbol{u} \in \mathbb{Z}^s$. Then either (i) P has an associate $Q \in \mathcal{R}$ such that $Q = \overline{Q}$, or (ii) there exists $Q \in \mathcal{R}$ such that $P = Q + \boldsymbol{z}^{\boldsymbol{u}}\overline{Q}$ and P does not divide Q in $\mathcal{R}$.*

Proof. Consider a monomial M such that $\boldsymbol{z}^{\boldsymbol{u}}\overline{M} = M$. Then M has a real coefficient and the exponent $\boldsymbol{w}$ of $\boldsymbol{z}$ in M satisfies $2\boldsymbol{w} = \boldsymbol{u}$. Thus if $\boldsymbol{z}^{\boldsymbol{u}}\overline{M} = M$ for every monomial M appearing in P then P has the form $Q\boldsymbol{z}^{\boldsymbol{w}}$, where $2\boldsymbol{w} = \boldsymbol{u}$ and Q is a polynomial in the variables x and $\boldsymbol{y}$ with real coefficients. In particular $Q = \overline{Q}$, and statement (i) of the proposition applies.

Suppose now that $\boldsymbol{z}^{\boldsymbol{u}}\overline{M} \neq M$ for some monomial M appearing in P. Then the map sending M to $\boldsymbol{z}^{\boldsymbol{u}}\overline{M}$ induces a permutation of order 2 on the monomials on P. Thus we may write $P = \sum_{j=1}^{n} M_j$, where $n = k + 2\ell$ for some $k \geq 0$ and $\ell \geq 1$ such that $\boldsymbol{z}^{\boldsymbol{u}}\overline{M_j} = M_j$ for $1 \leq j \leq k$ and $\boldsymbol{z}^{\boldsymbol{u}}\overline{M_j} = M_{j+\ell}$ for $k+1 \leq j \leq \ell$. Then, writing $Q := \frac{1}{2}\sum_{j=1}^{k} M_j + \sum_{j=k+1}^{k+\ell} M_j$, we have $P = Q + \boldsymbol{z}^{\boldsymbol{u}}\overline{Q}$.

The set of monomials appearing in Q is a proper subset of the set of monomials appearing in P (up to constant coefficients). Thus Q cannot be a constant multiple of P. Furthermore for each variable $\sigma \in \{x, y_j, z_k : 1 \leq j \leq r, 1 \leq k \leq s\}$, the maximum degree of σ in P is at least its maximum degree in Q, and likewise for σ^{-1}. It follows that Q cannot be a multiple of P by a non-constant polynomial. We conclude that P does not divide Q. □

2.4 Schanuel's Conjecture

The main result of this section depends on Schanuel's conjecture, one of the central conjectures in transcendental number theory [14], which, if true, generalises most known results in the field. Recall that a *transcendence basis* of a field extension $L : K$ is a subset $S \subseteq L$ that is algebraically independent over K and such that L is algebraic over $K(S)$. All transcendence bases of $L : K$ have the same cardinality, which is called the *transcendence degree* of the extension.

Conjecture 2 (Schanuel's Conjecture [14]) *Let $a_1, \ldots, a_n$ be complex numbers that are linearly independent over $\mathbb{Q}$. Then the extension*

$$\mathbb{Q}(a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n}) : \mathbb{Q}$$

has transcendence degree at least n.

A special case of Schanuel's conjecture, that is known to be true, is the Lindemann Weierstrass Theorem: if $a_1, \ldots, a_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then $e^{a_1}, \ldots, e^{a_n}$ are algebraically independent.

We apply Schanuel's conjecture via the following proposition.

Proposition 3. *Let $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ be $\mathbb{Q}$-linearly independent sets of real algebraic numbers. Furthermore, let $P, Q \in \mathcal{R}$ be two polynomials that have algebraic coefficients and are coprime in $\mathcal{R}$. Then the equations*

$$P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) = 0 \tag{2}$$

$$Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) = 0 \tag{3}$$

have no non-zero solution $t \in \mathbb{R}$.

Proof. Consider a solution $t \neq 0$ of Equations (2) and 3. By passing to suitable associates, we may assume without loss of generality that P and Q lie in $\mathcal{A}$, i.e., that all variables in P and Q appear with non-negative exponent. Moreover, since P and Q are coprime in $\mathcal{R}$, their greatest common divisor R in $\mathcal{A}$ is a monomial. In particular,

$$R(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) \neq 0\,.$$

Thus, dividing P and Q by R, we may assume that P and Q are coprime in $\mathcal{A}$ and that Equations (2) and 3 still hold.

By Schanuel's conjecture, the extension

$$\mathbb{Q}(a_1 t, \dots, a_r t, ib_1 t, \dots, ib_s t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) : \mathbb{Q}$$

has transcendence degree at least $r+s$. Since $a_1, \dots, a_r$ and $b_1, \dots, b_s$ are algebraic over $\mathbb{Q}$, writing

$$S := \langle t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t} \rangle \,,$$

it follows that the extension $\mathbb{Q}(S) : \mathbb{Q}$ also has transcendence degree at least $r+s$.

From Equations (2) and (3) we can regard S as specifying a common root of P and Q. Pick some variable $\sigma \in \{x, y_j, z_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ that has positive degree in P. Then the component of S corresponding to σ is algebraic over the remaining components of S. We claim that the remaining components of S are algebraically dependent and thus S comprises at most $r+s-1$ algebraically independent elements, contradicting Schanuel's conjecture. The claim clearly holds if σ does not appear in Q. On the other hand, if σ has positive degree in Q then, since P and Q are coprime polynomials, the multivariate resultant $\mathrm{Res}_\sigma(P, Q)$ is a non-zero polynomial in the set of variables $\{x, y_j, z_j : 1 \leq i \leq r, 1 \leq j \leq s\} \setminus \{\sigma\}$ which has a root at S (see, e.g., [7, Page 163]). Thus the claim also holds in this case. In either case we obtain a contradiction to Schanuel's conjecture and we conclude that Equations (2) and (3) have no non-zero solution $t \neq 0$. □

3 Decidability of the Bounded Skolem Problem

Let $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_s\}$ be $\mathbb{Q}$-linearly independent sets of real algebraic numbers and consider the exponential polynomial

$$f(t) = P(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) \,, \tag{4}$$

where $P \in \mathcal{R}$ is irreducible. We say that f is a *Type-1* exponential polynomial if P and $\overline{P}$ are not associates in $\mathcal{R}$, we say that f is *Type-2* if $P = \alpha \overline{P}$ for some $\alpha \in \mathbb{C}$, and we say that f is *Type-3* if $P = U\overline{P}$ for some non-constant unit $U \in \mathcal{R}$. These three cases are mutually exhaustive by construction.

Example 4. The simplest example of a Type-3 exponential polynomial is $g(t) = 1 + e^{it}$. Here $g(t) = P(e^{it})$, where $P(z) = 1+z$ is an irreducible polynomial that is associated with its conjugate $\overline{P}(z) = 1 + z^{-1}$. Note that the exponential polynomial $f(t) = 2 + \cos(t)$ from the Introduction factors as the product of two type-3 exponential polynomials $f(t) = g(t)\overline{g(t)}$.

In the case of a Type-2 exponential polynomial $P = \alpha\overline{P}$ it is clear that we must have $|\alpha| = 1$. Moreover, by replacing P by βP, where $\beta^2 = \overline{\alpha}$, we may assume without loss of generality that $P = \overline{P}$. Similarly, in the case of a Type-3 exponential polynomial, we can assume without loss of generality that $P = \boldsymbol{z}^{\boldsymbol{u}}\overline{P}$ for some non-zero vector $\boldsymbol{u} \in \mathbb{Z}^s$.

Now consider an arbitrary exponential polynomial $f(t) := \sum_{j=1}^{n} P_j(t) e^{\lambda_j t}$. Let $\{a_1, \dots, a_r\}$ be a basis of the $\mathbb{Q}$-vector space spanned by $\{\Re(\lambda_j) : 1 \leq j \leq n\}$ and let $\{b_1, \dots, b_s\}$ be a basis of the the $\mathbb{Q}$-vector space spanned by $\{\Im(\lambda_j) : 1 \leq j \leq n\}$. Without loss of generality we may assume that each characteristic root λ is an integer linear combination of $a_1, \dots, a_r$ and $ib_1, \dots, ib_s$. Then $e^{\lambda t}$ is a product of positive and negative powers of $e^{a_1 t}, \dots, e^{a_r t}$ and $e^{ib_1 t}, \dots, e^{ib_s t}$. It follows that there is a Laurent polynomial $P \in \mathcal{R}$ such that

$$f(t) = P(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) \,. \tag{5}$$

Since P can be written as a product of irreducible factors, it follows that f can be written as product of Type-1, Type-2, and Type-3 exponential polynomials, and moreover this factorisation can be computed from f. Thus it suffices to show how to decide the existence of zeros of these three special forms of exponential polynomial. We will handle all three cases using Schanuel's conjecture.

Theorem 5. *The Bounded Continuous Skolem Problem is decidable subject to Schanuel's conjecture.*

Proof. Consider an exponential polynomial

$$f(t) = P(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t})\,, \tag{6}$$

where $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_s\}$ are $\mathbb{Q}$-linearly independent sets of real algebraic numbers, and $P \in \mathcal{R}$ is irreducible. We show how to decide whether f has a zero in a bounded interval $I \subseteq \mathbb{R}_{\geq 0}$, considering separately the case of Type-1, Type-2, and Type-3 exponential polynomials.

If $f(t) = 0$ and t is algebraic then $e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}$ are algebraically dependent over $\mathbb{Q}$. But this is impossible unless $t = 0$ by the Lindemann Weierstrass. Thus $f(t) \neq 0$ for any non-zero rational number t and it is no loss of generality to assume that $I = (c, d)$ is an open interval.

Case (i): *f* is Type-1

By assumption, P and $\overline{P}$ are not associates in (6) and are therefore coprime. We claim that in this case the equation $f(t) = 0$ has no solution $t \in \mathbb{R}$. Indeed $f(t) = 0$ implies

$$\begin{aligned} P(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) &= 0 \\ \overline{P}(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) &= 0\,, \end{aligned}$$

and the non-existence of a zero of f follows immediately from Proposition 3.

Case (ii): *f* is Type-2

In this case we have $P = \overline{P}$ in (6) and so f is real-valued. It will suffice to show that the equations $f(t) = f'(t) = 0$ have no solution $t \in \mathbb{R}$, for then we can use the procedure of Section 2.1 to determine whether or not f has a zero in (c, d).

We can write $f'(t)$ in the form

$$f'(t) = Q(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t})\,,$$

where Q is the polynomial

$$Q = \frac{\partial P}{\partial x_0} + \sum_{j=1}^{r} a_j x_j \frac{\partial P}{\partial x_j} + \sum_{j=1}^{s} i b_j z_j \frac{\partial P}{\partial z_j}\,.$$

We claim that P and Q are coprime. Indeed, since P is irreducible, P and Q can only fail to be coprime if P divides Q.

If P has strictly positive degree d in x then Q has degree $d-1$ in x and thus P cannot divide Q. On the other hand, if P has degree 0 in x then Q is obtained from P by multiplying each monomial $\boldsymbol{y}^{\boldsymbol{u}}\boldsymbol{z}^{\boldsymbol{v}}$ appearing in P by the constant $\sum_{j=1}^{r} a_j u_j + i \sum_{j=1}^{s} b_j v_j$. Moreover, by the assumption of linear independence of $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_s\}$, each monomial in P is multiplied by a different constant. Since P is not a unit it has at least two different monomials and so P is not a constant multiple of Q. Furthermore, for each variable $\sigma \in \{y_j, y_j^{-1} : 1 \leq j \leq r\} \cup \{z_j, z_j^{-1} : 1 \leq j \leq s\}$, the degree of σ in P is at least the degree of σ in Q. Thus P cannot be a multiple of Q by a non-constant polynomial.

We conclude that P does not divide Q and hence P and Q are coprime. It now follows from Proposition 3 that the equations $f(t) = f'(t) = 0$ have no solution $t \in \mathbb{R}$.

Case (iii): f is Type-3

Suppose that f is a Type-3 exponential polynomial. Then in (6) we have that $P = \boldsymbol{z}^{\boldsymbol{u}}\overline{P}$ for some non-zero vector $\boldsymbol{u} \in \mathbb{Z}^s$. By Proposition 1 we can write $P = Q + \boldsymbol{z}^{\boldsymbol{u}}\overline{Q}$ for some polynomial $Q \in \mathcal{R}$ that is coprime with P.

Now define

$$g_1(t) := Q(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t})$$

and $g_2(t) := e^{ib_1 u_1} \dots e^{ib_s u_s}\overline{g_1(t)}$, so that $f(t) = g_1(t) + g_2(t)$ for all t.

We show that $g_2(t) \neq 0$ for all $t \in \mathbb{R}$. Indeed if $g_2(t) = 0$ for some t then we also have $g_1(t) = 0$ and hence $f(t) = 0$. For such a t it follows that

$$\begin{aligned} P(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) &= 0 \\ Q(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) &= 0\,. \end{aligned}$$

But P and Q are coprime and so these two equations cannot both hold by Proposition 3. Not only do we have $g_2(t) \neq 0$ for all $t \in \mathbb{R}$, but, applying the sampling procedure in Section 2.1 to $|g_2(t)|^2$ we can compute a strictly positive lower bound on $|g_2(t)|$ over the interval (c, d).

Since $g_2(t) \neq 0$ for all $t \in \mathbb{R}$ we may define the function $h : (c, d) \to \mathbb{R}$ by

$$h(t) := i \log\left(\frac{g_1(t)}{g_2(t)}\right) + \pi\,.$$

Note that $h(t) = 0$ if and only if $f(t) = 0$. Our aim is to use the procedure of Section 2.1 to decide the existence of a zero of h in the interval (c, d), and thus decide whether f has a zero in (c, d). To this end, we first observe that using the strictly positive lower bound on $|g_2(t)|$ over the interval (c, d), obtained above, we can compute an upper bound on $|h'(t)|$ on (c, d). It remains to show that h has no tangential zeros in this interval.

Now let $t \in (c, d)$ be such that $h(t) = 0$. Then $g_1(t) = -g_2(t)$. Moreover for such t, recalling that $g_2(t) \neq 0$, we have

$$\begin{aligned} h'(t) = 0 \quad &\text{iff} \quad \frac{g_2(t)}{g_1(t)} \, \frac{g_1'(t)g_2(t) - g_2'(t)g_1(t)}{g_2(t)^2} = 0 \\ &\text{iff} \quad g_1'(t)g_2(t) - g_2'(t)g_1(t) = 0 \\ &\text{iff} \quad g_1'(t)g_2(t) + g_2'(t)g_2(t) = 0 \\ &\text{iff} \quad g_1'(t) + g_2'(t) = 0 \\ &\text{iff} \quad f'(t) = 0\,. \end{aligned}$$

Thus $h(t) = h'(t) = 0$ implies $f(t) = f'(t) = 0$. But the proof in Case (ii) shows that $f(t) = f'(t) = 0$ is impossible. (Nothing in that argument hinges on f being real-valued.) Thus h has no tangential zeros and this concludes the proof. □

4 The Unbounded Case

In this section we show that decidability of the Continuous Skolem Problem entails significant new effectiveness results in Diophantine approximation, thereby identifying a formidable mathematical obstacle to further progress in the unbounded case.

Diophantine approximation is a branch of number theory concerned with approximating real numbers by rationals. A central role is played in this theory by the notion of *continued fraction expansion*, which allows to compute a sequence of rational approximations to a given real number that is optimal in a certain well-defined sense. For our purposes it suffices to note that the behaviour of the continued fraction expansion of a real number a is closely related the *(homogeneous Diophantine approximation) type* of a, which is defined to be

$$L(a) := \inf \left\{ c : \left| a - \frac{n}{m} \right| < \frac{c}{m^2} \text{ for some } m, n \in \mathbb{Z} \right\} .$$

If a has simple continued fraction expansion $a = [n_1, n_2, n_3, \ldots]$, then, writing $K(a) := \sup_{k \geq 0} n_k$, it is shown in [18, pp. 22-23] that $L(a) = 0$ if and only if $K(a)$ is infinite and otherwise

$$K(a) \leq L(a)^{-1} \leq K(a) + 2 \,.$$

It is well known that a real number algebraic number of degree two over the rationals has a continued fraction expansion that is ultimately periodic. In particular, such numbers have bounded partial quotients. But nothing is known about real algebraic numbers of degree three or more—no example is known with bounded partial quotients, nor with unbounded quotients. Guy [9] asks:

> *Is there an algebraic number of degree greater than two whose simple continued fraction expansion has unbounded partial quotients? Does every such number have unbounded partial quotients?*

In other words, the question is whether there is a real algebraic number a of degree at least three such that $L(a)$ is strictly positive, or whether $L(a) = 0$ for all such a.

Recall that a real number x is *computable* if there is an algorithm which, given any rational $\varepsilon > 0$ as input, returns a rational q such that $|q - x| < \varepsilon$. The main result of this section is Theorem 9, which shows that the existence of a decision procedure for the general Continuous Skolem Problem entails the computability of $L(a)$ for all real algebraic numbers a. Now one possibility is that all such numbers $L(a)$ are zero, and hence trivially computable. However the significance of Theorem 9 is that in order to prove the decidability of the Continuous Skolem Problem one would have to establish, *one way or another*, the computability of $L(a)$ for every real algebraic number a.

Fix positive $a, c \in \mathbb{R} \cap \mathbb{A}$ and define the functions:

$$\begin{aligned} f_1(t) &= e^t(1 - \cos(t)) + t(1 - \cos(at)) - c\sin(at), \\ f_2(t) &= e^t(1 - \cos(t)) + t(1 - \cos(at)) + c\sin(at), \\ f(t) &= e^t(1 - \cos(t)) + t(1 - \cos(at)) - c|\sin(at)| = \min\{f_1(t), f_2(t)\}. \end{aligned}$$

Then $f_1(t)$ and $f_2(t)$ are exponential polynomials. Moreover it is easy to check that the function $f(t)$ has a zero in an interval of the form (T, ∞) if and only if at least one of $f_1(t)$, $f_2(t)$ has a zero in (T, ∞).

We will first prove two lemmas which show a connection between the existence zeros of $f(t)$ and the type $L(a)$. We then will derive an algorithm to compute $L(a)$ using an oracle for the Continuous Skolem Problem, thereby demonstrating our desired hardness result.

Lemma 6. *Fix $a, c \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon \in \mathbb{Q}$ with $a, c > 0$ and $\varepsilon \in (0, 1)$. There exists an effective threshold T, dependent on a, c, ε, such that if $f(t) = 0$ for some $t \geq T$, then $L(a) \leq c/2\pi^2(1 - \varepsilon)$.*

Proof. Suppose $f(t) = 0$ for some $t \geq T$. Define $\delta_1 = t - 2\pi m$ and $\delta_2 = at - 2\pi n$, where $m, n \in \mathbb{N}$ and $\delta_1, \delta_2 \in [-\pi, \pi)$. Then we have

$$\left| a - \frac{n}{m} \right| = \frac{|\delta_2 - a\delta_1|}{2\pi m}.$$

We will show that for T chosen large enough, if $f(t) = 0$ for $t \geq T$ then we can bound $|\delta_2|$ and $|a\delta_1|$ separately from above and then apply the triangle inequality to bound $|\delta_2 - a\delta_1|$, obtaining the desired upper bound on $L(a)$.

Define $0 < \alpha < 1$ by $\alpha^2 = (1 - \varepsilon^2)$. Since $m \geq \dfrac{t - \pi}{2\pi} \geq \dfrac{T - \pi}{2\pi}$, for sufficiently large T we have

$$t \geq 2\pi(m - 1) \geq 2\pi m\alpha\,. \tag{7}$$

Furthermore, since $\alpha x^2/2 \leq 1 - \cos(x)$ for $|x|$ sufficiently small, we may assume that T is large enough such that the following is valid for $|x| \leq \pi$:

$$\text{if } 1 - \cos(x) \leq c\pi/T \text{ then } \alpha x^2/2 \leq 1 - \cos(x). \tag{8}$$

We have the following chain of inequalities, where $(*)$ follows from $f(t) = 0$ and $e^t(1-\cos(t)) \geq 0$:

$$1 - \cos(\delta_2) = 1 - \cos(at) \overset{(*)}{\leq} \frac{c|\sin(at)|}{t} = \frac{c|\sin(\delta_2)|}{t} \leq \frac{c|\delta_2|}{t}\,.$$

It follows that $1 - \cos(\delta_2) \leq c\pi/t$ and so by (8) we also have

$$\frac{\alpha\delta_2^2}{2} \leq 1 - \cos(\delta_2)\,.$$

Combining the upper and lower bounds on $1 - \cos(\delta_2)$ and using (7), we have

$$|\delta_2| \leq \frac{2c}{\alpha t} \leq \frac{2c}{2\pi m\alpha^2} = \frac{c}{m\pi(1 - \varepsilon^2)}.$$

We next seek an upper bound on $|\delta_1|$. To this end, let T be large enough so that

$$ce^{-t} \leq \left(\frac{c\varepsilon}{2a\alpha t}\right)^2 \quad \text{for } t \geq T. \tag{9}$$

Then the following chain of inequalities holds:

$$\begin{aligned}
\frac{\delta_1^2}{16} &\leq 1 - \cos(\delta_1) && \{ \text{ valid for all } |\delta_1| \leq \pi \ \} \\
&= \frac{c|\sin(\delta_2)| - t(1 - \cos(\delta_2))}{e^t} && \{ \text{ since } f(t) = 0 \ \} \\
&\leq ce^{-t} && \{ \text{ since } |\sin(\delta_2)|, |\cos(\delta_2)| \leq 1 \} \\
&\leq \left(\frac{c\varepsilon}{2a\alpha t}\right)^2 && \{ \text{ by (9) } \} \\
&\leq \left(\frac{c\varepsilon}{4a\pi\alpha^2 m}\right)^2 && \{ \text{ by (7) } \}
\end{aligned}$$

It follows that

$$|a\delta_1| \leq \frac{c\varepsilon}{\pi m(1 - \varepsilon^2)}\,.$$

Finally, by the triangle inequality and the bounds on $|a\delta_1|$ and $|\delta_2|$, we have

$$\left|a - \frac{n}{m}\right| = \frac{|\delta_2 - a\delta_1|}{2\pi m} \leq \frac{|\delta_2| + |a\delta_1|}{2\pi m} \leq \frac{c + c\varepsilon}{2\pi^2 m^2(1 - \varepsilon^2)} = \frac{c}{2\pi^2 m^2(1 - \varepsilon)}\,,$$

so the natural numbers n, m witness $L(a) \leq c/2\pi^2(1 - \varepsilon)$. □

Lemma 7. *Fix $a, c \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon \in \mathbb{Q}$ with $a, c > 0$ and $\varepsilon \in (0, 1)$. There exists an effective threshold M, dependent on a, c, ε, such that if $L(a) \leq c(1 - \varepsilon)/2\pi^2$ holds and is witnessed by natural numbers n, m with $m \geq M$, then $f(t) = 0$ for some $t \geq 2\pi M$.*

Proof. Select M large enough, so that $c(1-\varepsilon)/\pi M < \pi$ and

$$\text{if } |x| < c(1-\varepsilon)/\pi M, \text{ then } (1-\varepsilon)|x| \leq |\sin(x)|. \tag{10}$$

Suppose now that $L(a) \leq c(1-\varepsilon)/2\pi^2$, let this be witnessed by $n, m \in \mathbb{N}$ with $m \geq M$ and define $t := 2\pi m$. We will show that $f(t) \leq 0$. This suffices, because $f(t)$ is continuous and moreover is positive for arbitrarily large times, so it must have a zero on $[t, \infty)$.

Since $L(a) \leq c(1-\varepsilon)/2\pi^2$, we have $|am - n| \leq c(1-\varepsilon)/2\pi^2 m$. Therefore, we can write $at = 2\pi am = 2\pi n + \delta$ for some δ satisfying $|\delta| \leq c(1-\varepsilon)/\pi m < \pi$. We have

$$\begin{aligned}
& f(t) \\
= & \{ \text{ as } \cos(t) = 1 \ \} \\
& t(1-\cos(\delta)) - c|\sin(\delta)| \\
\leq & \{ \text{ by (10) and } 1-\cos(x) \leq x^2/2 \ \} \\
& \pi m \delta^2 - c(1-\varepsilon)|\delta| \\
\leq & \{ \text{ by } |\delta| \leq c(1-\varepsilon)/\pi m \ \} \\
& 0.
\end{aligned}$$

□

The following corollary is immediate:

Lemma 8. *Fix $a, c \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon \in \mathbb{Q}$ with $a, c > 0$ and $\varepsilon \in (0,1)$. There exists an effective threshold T, dependent on a, c, ε, such that if $f(t) \neq 0$ for all $t \geq T$, then either $L(a) < c(1-\varepsilon)/2\pi^2$ and this is witnessed by natural numbers n, m with $m < T/2\pi$, or $L(a) \geq c(1-\varepsilon)/2\pi^2$.*

We now use the above lemmas to show the central result of this section:

Theorem 9. *Fix a positive real algebraic number a. If the Continuous Skolem Problem is decidable then $L(a)$ may be computed to within arbitrary precision.*

Proof. Suppose we know $L(a) \in [p, q]$ for non-negative $p, q \in \mathbb{Q}$. Choose $c \in \mathbb{R} \cap \mathbb{A}$ with $c > 0$ and a rational $\varepsilon \in (0,1)$ such that

$$p < \frac{c(1-\varepsilon)}{2\pi^2} < \frac{c}{2\pi^2(1-\varepsilon)} < q.$$

Write $A := c(1-\varepsilon)/2\pi^2$ and $B := c/2\pi^2(1-\varepsilon)$. Calculate the maximum of the thresholds T required by Lemmas 6 and 8. Check for all denominators $m \leq T/2\pi$ whether there exists a numerator n such that n, m witness $L(a) \leq A$. If so, then continue the approximation procedure recursively with confidence interval $[p, A]$. Otherwise, use the oracle for the Continuous Skolem Problem to determine whether at least one of $f_1(t), f_2(t)$ has a zero on $[T, \infty)$. If this is the case, then $f(t)$ also has a zero on $[T, \infty)$, so by Lemma 6, $L(a) \leq B$ and we continue the approximation recursively on the interval $[p, B]$. If not, then $L(a) \geq A$ by Lemma 8, so we continue on the interval $[A, q]$. Notice that in this procedure, one can choose c, ε at each stage in such a way that the confidence interval shrinks by at least a fixed factor, whatever the outcome of the oracle invocations. It follows therefore that $L(a)$ can be approximated to within arbitrary precision. □

References

1. R. Alur, *Principles of Cyber-Physical Systems*, MIT Press, 2015.
2. P. C. Bell, J.-C. Delvenne, R. M. Jungers, and V. D. Blondel, *The Continuous Skolem-Pisot Problem*, Theoretical Computer Science, 411 (2010), pp. 3625–3634.

3. R. P. Brent, *Fast multiple-precision evaluation of elementary functions*, J. ACM, 23 (1976), pp. 242–251.
4. T. Chen, N. Yu, and T. Han, *Continuous-time orbit problems are decidable in polynomial-time*, Inf. Process. Lett., 115 (2015), pp. 11–14.
5. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.
6. P. M. Cohn, *Basic Algebra: Groups, Rings and Fields*, Springer, 2002.
7. D. A. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 2007.
8. P. D'Aquino, A. Macintyre, and G. Terzo, *From Schanuel's conjecture to Shapiro's conjecture*, Comment. Math. Helv., 89 (2014), pp. 597–616.
9. R. Guy, *Unsolved Problems in Number Theory*, Springer, third ed., 2004.
10. E. Hainry, *Reachability in linear dynamical systems*, in Logic and Theory of Algorithms, Springer, 2008, pp. 241–250.
11. V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki, *Skolem's Problem – on the border between decidability and undecidability*, Tech. Rep. 683, Turku Centre for Computer Science, 2005.
12. E. Kaltofen, *Polynomial factorization*, in (B. Buchberger, G. Collins, and R. Loos, editors) Computer Algebra, Springer, 1982, pp. 95–113.
13. G. Lafferriere, G. J. Pappas, and S. Yovine, *Symbolic reachability computation for families of linear vector fields*, J. Symb. Comput., 32 (2001), pp. 231–253.
14. S. Lang, *Introduction to transcendental numbers*, Reading, Mass, (1966).
15. A. Macintyre and A. J. Wilkie, *On the decidability of the real exponential field*, (1996).
16. J. Ouaknine and J. Worrell, *Positivity problems for low-order linear recurrence sequences*, in Proceedings of SODA, 2014, pp. 366–379.
17. V. Pan, *Optimal and nearly optimal algorithms for approximating polynomial zeros*, Computers and Mathematics with Applications, 31 (1996), pp. 97 – 138.
18. W. Schmidt, *Diophantine approximation*, 785 (1980).
19. T. Tao, *Structure and randomness: pages from year one of a mathematical blog*, American Mathematical Society, 2008.
20. B. Zilber, *Exponential sums equations and the Schanuel conjecture*, Journal of the London Mathematical Society, 65 (2002), pp. 27–44.