On the Skolem Problem for Continuous Linear Dynamical Systems

Ventsislav Chonev[1], Joël Ouaknine[2], and James Worrell[2]

1 **Institute of Science and Technology, Austria**
2 **University of Oxford, UK**

Abstract

The Continuous Skolem Problem asks whether a real-valued function satisfying a linear differential equation has a zero in a given interval of real numbers. This is a fundamental reachability problem for continuous linear dynamical systems, such as linear hybrid automata and continuous-time Markov chains. Decidability of the problem is currently open; indeed 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 unifying conjecture in transcendental number theory. We furthermore analyse the unbounded problem in terms of the frequencies of the differential equation, that is, the imaginary parts of the characteristic roots. We give a reduction of the unbounded problem to the bounded problem in the case of at most one rationally linearly independent frequency or two rationally linearly independent frequencies and simple characteristic roots. We complete the picture by showing that decidability of the unbounded problem in the case of two (or more) rationally linearly independent frequencies would entail a major new effectiveness result in Diophantine approximation, namely computability of the Diophantine-approximation types of all real algebraic numbers.

1998 ACM Subject Classification F.1.1 Models of Computation, F.2.1 Numerical Algorithms and Problems

Keywords and phrases keywords

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

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 and 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 [4, 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

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 1–19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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 given hyperplane $\{\boldsymbol{y} \in \mathbb{R}^n : \boldsymbol{u}^T\boldsymbol{y} = 0\}$ with normal vector $\boldsymbol{u} \in \mathbb{R}^n$. 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), and it turns out that the hyperplane reachability problem is inter-reducible with the Continuous Skolem Problem (see [4, Theorem 6] for further details). Moreover, under this reduction the Bounded Continuous Skolem Problem corresponds to a time-bounded version of the hyperplane reachability problem.

The *characteristic polynomial* of the 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 $f(t) = \sum_{j=1}^{m} P_j(t)e^{\lambda_j t}$, where the P_j are polynomials with algebraic coefficients that are determined by the initial conditions of the differential equation. We call a function f in this form an *exponential polynomial*. If the roots of χ are all simple then f can be written as an exponential polynomial in which the polynomials P_j are all constant.

The Continuous Skolem Problem can equivalently be formulated in terms of whether an exponential polynomial has a zero in a given interval of reals. If the characteristic roots have the form $\lambda_j = r_j + i\omega_j$, where $r_j, \omega_j \in \mathbb{R}$, then we can also write $f(t)$ in the form $f(t) = \sum_{j=1}^{m} e^{r_j t}(Q_{1,j}(t)\sin(\omega_j t) + Q_{2,j}(t)\cos(\omega_j t))$, where the polynomials $Q_{1,j}, Q_{2,j}$ have real-algebraic coefficients. We call $\omega_1, \ldots, \omega_m$ the *frequencies* of f.

Our first result is to show decidability of the Bounded Continuous Skolem Problem subject to Schanuel's Conjecture, a unifying conjecture in transcendental number theory that plays a key role in the study of real and complex exponentials [21]. Intuitively, decidability of the Bounded Continuous Skolem Problem is non-trivial because an exponential polynomial can approach 0 tangentially. However, 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 we do not obtain a complexity bound for the procedure.

A celebrated paper of Macintyre and Wilkie [16] obtains decidability of the first-order theory of $\mathbb{R}_{\exp} = (\mathbb{R}, 0, 1, <, \cdot, +, \exp)$ assuming Schanuel's Conjecture over $\mathbb{R}$. The proof of [15, Theorem 3.1] mentions an unpublished result of Macintyre and Wilkie that generalise [16] to obtain decidability when $\mathbb{R}_{\exp}$ is augmented with the functions $\sin\restriction_{[0,2\pi]}$ and $\cos\restriction_{[0,2\pi]}$, this time assuming Schanuel's Conjecture over $\mathbb{C}$. Such a result would immediately imply (conditional) decidability of the Bounded Continuous Skolem Problem. However the latter decidability result is simpler and, as we show below, can be established more directly.

In the unbounded case we analyse exponential polynomials in terms of the number of rationally linearly independent frequencies. We give a reduction of the unbounded problem to the bounded problem in the case of at most one rationally linearly independent frequency and in the case of two rationally linearly independent frequencies with all characteristic roots simple. These two results are unconditional and rely on the cell decomposition theorem for semi-algebraic sets as well as Diophantine-approximation lower bounds for logarithms of algebraic numbers.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 2–19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

We complete the picture by showing that decidability of the unbounded problem in the case of two (or more) rationally linearly independent frequencies would entail a major new effectiveness result in Diophantine approximation—namely computability of the Diophantine-approximation types of all real algebraic numbers. As we discuss in Appendix B, currently essentially nothing is known about Diophantine-approximation types of algebraic numbers of degree three or higher, and they are the subject of several longstanding open problems.

The question of deciding whether an exponential polynomial f has infinitely many zeros is investigated in [6]. There the problem is shown to be decidable if f satisfies a differential equation of order at most 7. This result does not rely on Schanuel's Conjecture. For the general case of the infinite zeros problem there is a hardness result of a similar flavour to that in Appendix B.

2 Mathematical Background

2.1 Zero Finding

Let $f : [a, b] \to \mathbb{R}$ be a function defined on a closed interval of reals with endpoints $a, b \in \mathbb{Q}$. Suppose the following two conditions hold: (i) there exists $M > 0$ such that f is M-Lipschitz, i.e., $|f(s) - f(t)| \leq M|s - t|$ for all $s, t \in [a, b]$; (ii) given $t \in [a, b] \cap \mathbb{Q}$ and positive error bound $\varepsilon \in \mathbb{Q}$, we can compute $q \in \mathbb{Q}$ such that $|f(t) - q| < \varepsilon$. Then given a positive rational number δ we can compute piecewise linear functions $f_\delta^+, f_\delta^- : [a, b] \to \mathbb{R}$ such that $f_\delta^-(t) \leq f(t) \leq f_\delta^+(t)$ and $f_\delta^+(t) - f_\delta^-(t) \leq \delta$ for all $t \in [a, b]$. We do this as follows:

1. Pick $N \in \mathbb{N}$ such that $\frac{1}{N} < \frac{\delta}{4(b-a)M}$ and consider sample points $s_j := \frac{ja+(N-j)b}{N}$, $j = 0, \ldots, N$, dividing the interval $[a, b]$ into N sub-intervals, each of length at most $\frac{\delta}{4M}$.
2. For each sample point s_j compute $q_j \in \mathbb{Q}$ such that $|q_j - f(s_j)| < \frac{\delta}{4}$, define $f_\delta^-(s_j) = q_j - \frac{\delta}{2}$, $f_\delta^+(s_j) = q_j + \frac{\delta}{2}$, and extend f_δ^- and f_δ^+ linearly between sample points.

Now suppose that f satisfies the following additional conditions: (iii) $f(a) \neq 0, f(b) \neq 0$; (iv) for any $t \in (a, b)$ such that $f(t) = 0$, $f'(t)$ exists and is non-zero, i.e., f has no tangential zeros. Then we can decide the existence of a zero of f by computing upper and lower approximations f_δ^+ and f_δ^- for successively smaller values of δ. If $f_\delta^+(t) < 0$ for all t or $f_\delta^-(t) > 0$ for all t then we conclude that f has no zero on $[a, b]$; if $f_\delta^+(s) < 0$ and $f_\delta^-(t) > 0$ for some s, t then we conclude that f has a zero; otherwise we proceed to a smaller value of δ. This procedure terminates since by (iii) and (iv) either f has a zero in $[a, b]$ or it is bounded away from zero.

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 [7, 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 [7, Section 4.5.4].

Given the characteristic polynomial χ of a linear differential equation, we can compute approximations of each of its roots $\lambda_1, \ldots, \lambda_m$ to within an arbitrarily small additive error [17]. One can then compute a primitive element θ of the extension field $\mathbb{Q}(\lambda_1, \ldots, \lambda_m)$ together with a representation of each characteristic root λ_j as a polynomial $\lambda_j = \sum_{k=0}^{d-1} q_{jk}\theta^k$ in θ with rational coefficients q_{jk}, where d is the degree of θ (e.g., see [20]). Then for an integer

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 3–19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

vector $(c_1, \ldots, c_m) \in \mathbb{Z}^m$ we have $\sum_{j=1}^{m} c_j \lambda_j = 0$ if and only if $\sum_{j=1}^{m} c_j q_{jk}$ for $k = 0, \ldots, d-1$. Thereby we can determine maximal $\mathbb{Q}$-linearly independent subsets of $\{\mathrm{Re}(\lambda_j) : 1 \leq j \leq m\}$ and $\{\mathrm{Im}(\lambda_j) : 1 \leq j \leq m\}$.

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 [5].

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 [8, 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 [13].

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 characterising polynomials in $P \in \mathcal{R}$ such that P and $\overline{P}$ are associates. 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 $z_1^{u_1} \ldots z_s^{u_s}$. The proof of the proposition is in Appendix C.

▶ 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 the form $P = \boldsymbol{z}^{\boldsymbol{u}} Q$ for some $Q \in \mathcal{R}$ with $Q = \overline{Q}$, 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 $\mathcal{R}$.

2.4 Transcendence Theory

We will use transcendence theory in our analysis of both the bounded and unbounded variants of the Continuous Skolem Problem. In the unbounded case we will use the following classical result.

▶ **Theorem 2** (Gelfond-Schneider). *Let a, b be algebraic numbers not equal to 0 or 1. Then for any branch of the logarithm function, $\frac{\log(b)}{\log(a)}$ is either rational or transcendental.*

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 4–19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In fact we will make use of the following corollary, which is obtained by applying Theorem 2 to the algebraic numbers $a = e^{i(\alpha_2-\alpha_1)}$ and $b = e^{i(\beta_2-\beta_1)}$.

▶ **Corollary 3.** *Let $\alpha_1 \neq \beta_1$, $\alpha_2 \neq \beta_2$ all lie in $[0, \pi]$ and suppose that $\cos(\alpha_1), \cos(\alpha_2), \cos(\beta_1)$ and $\cos(\beta_2)$ are algebraic. Then $\frac{\beta_2-\alpha_2}{\beta_1-\alpha_1}$ is either rational or transcendental.*

Our results in the bounded case depend on Schanuel's conjecture, a unifying conjecture in transcendental number theory [14], which, if true, greatly generalises many of the central results in the field (including the Gelfond-Schneider Theorem, above). Recall that a *transcendence basis* of a field extension $L : K$ is a subset $S \subseteq L$ such that S is algebraically independent over K and 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 4 (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 hold unconditionally, 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, whose proof is in Appendix C.

▶ Proposition 5. 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

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

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

3 Decidability of the Bounded Skolem Problem

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

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

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 $U \in \mathcal{R}$.

▶ **Example 6.** 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 $\boldsymbol{u} \in \mathbb{Z}^s$.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 5–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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

$$f(t) = P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) \,. \tag{3}$$

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.

Writing the exponential polynomial $f(t)$ in (3) in the form $f(t) = \sum_{j=1}^{n} Q_j(t)e^{\lambda_j t}$, it follows from the irreducibility of P that the polynomials $Q_1, \ldots, Q_n$ have no common root. But then by the Lindemann-Weierstrass Theorem any zero of f must be transcendental (see [4, Theorem 8]).

▶ **Theorem 7.** *The Bounded Continuous Skolem Problem is decidable subject to Schanuel's conjecture.*

Proof. Consider an exponential polynomial

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

where $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ 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.

Case (i): f is Type-1

By assumption, P and $\overline{P}$ are both irreducible and are not associates 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

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

and the non-existence of a zero of f follows immediately from Proposition 5.

Case (ii): f is Type-2

In this case we have $P = \overline{P}$ and so f is real-valued. Our aim is to use the procedure of Section 2.1 to determine whether or not f has a zero in $[c, d]$. To this end, notice first that $f(c), f(d) \neq 0$ since any root of f must be transcendental. Moreover, since f' is bounded on $[c, d]$, f is Lipschitz on $[c, d]$. It remains to verify that the equations $f(t) = 0, f'(t) = 0$ have no common solution $t \in [c, d]$.

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

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

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 6–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

where Q is the polynomial

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

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 k in x then Q has degree $k-1$ 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 $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$, 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 5 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 (4) 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

$$g_1(t) := Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{i b_1 t}, \ldots, e^{i b_s t})$$

and $g_2(t) := e^{i b_1 u_1} \ldots e^{i b_s u_s} \overline{g_1(t)}$, 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

$$\begin{aligned} P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{i b_1 t}, \ldots, e^{i b_s t}) &= 0 \\ Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{i b_1 t}, \ldots, e^{i b_s t}) &= 0 . \end{aligned}$$

But P and Q are coprime and so these two equations cannot both hold by Proposition 5. 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 $|g_2(t)|^2$ (which is a differentiable function) 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

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

Notice 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 $[c, d]$.

Let $t \in (c, d)$ be such that $h(t) = 0$. Then $g_1(t) = -g_2(t)$ and so $\frac{g_1(t)}{g_2(t)} = -1$ does not lie

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 7–19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

on the branch cut of the logarithm function. It follows that h is differentiable at t and

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

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 in (c, d).

We cannot directly use the procedure in Section 2.1 to decide whether h has a zero in $[c, d]$ since h is not necessarily continuous: its value can jump from $-\pi$ to π (or *vice versa*) due to the branch cut of the logarithm along the positive real axis. However, due to the strictly positive lower bound on $|g_2(t)|$, the function $|h|$ *is* Lipschitz on $[c, d]$. Thus, applying the sampling procedure in Section 2.1 for computing lower and upper bounds of Lipschitz functions we can compute a set $E \subseteq [c, d]$ such that E is a finite union of intervals with rational endpoints, $|f(t)| \leq \frac{2\pi}{3}$ for $t \in E$, and $|f(t)| \geq \frac{\pi}{3}$ for $t \notin E$. In particular, E contains all zeros of f in $[c, d]$ and f is Lipschitz on E. Thus we can apply the zero-finding procedure from Section 2.1 to $h \restriction E$ and thereby decide whether or not h has a zero on $[c, d]$.

◀

4 The Unbounded Case

In this section we consider the unbounded case of the Continuous Skolem Problem. For our analysis it is convenient to present exponential polynomials in the form

$$f(t) = \sum_{j=1}^{n} e^{r_j t} \left(P_{1,j}(t)\cos(\omega_j t) + P_{2,j}(t)\sin(\omega_j t)\right)\,, \tag{5}$$

where r_j, ω_j are real algebraic numbers and $P_{1,j}, P_{2,j}$ are polynomials with real algebraic coefficients for $j = 1, \ldots, n$. Our aim is to classify the difficulty of the problem in terms of the number of rationally linear independent frequencies $\omega_1, \ldots, \omega_n$.

Recall that in Section 3 we have shown the bounded problem to be decidable subject to Schanuel's Conjecture. In Appendix A we give a reduction of the unbounded problem to the bounded problem in case the set of frequencies spans a one-dimensional vector space over $\mathbb{Q}$. In the present section we give a reduction of the unbounded problem to the bounded problem in case the set of frequencies spans a two-dimensional vector space over $\mathbb{Q}$ and the polynomials $P_{1,j}$ and $P_{2,j}$ are all constant. (This last condition is equivalent to the assumption that $f(t)$ is simple.) The argument in the two-dimensional case is a more sophisticated version of that in the one-dimensional case, although the result is not more general due the assumption of simplicity.

In Appendix B we present a family of instances showing that obtaining decidability of the unbounded problem in the two-dimensional case without the assumption of simplicity would require much finer Diophantine-approximation bounds than are currently known.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 8–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

4.1 Background on Semi-Algebraic Sets

A subset of $\mathbb{R}^n$ is *semi-algebraic* if it is defined by a Boolean combination of constraints of the form $P(x_1, \ldots, x_n) > 0$, where P is a polynomial with real algebraic coefficients. A partial function $f : \mathbb{R}^n \to \mathbb{R}$ is semi-algebraic if its graph is a semi-algebraic subset of $\mathbb{R}^{n+1}$. The Tarski-Seidenberg Theorem states that the semi-algebraic sets are closed under projection and are therefore precisely the first-order definable sets over the structure $(\mathbb{R}, <, +, \cdot, 0, 1)$.

Let $(i_1, \ldots, i_n)$ be a sequence of zeros and ones of length $n \geq 1$. An $(i_1, \ldots, i_n)$-*cell* is a subset of $\mathbb{R}^n$, defined by induction on n as follows:

(i) A (0)-cell is a singleton subset of $\mathbb{R}$ and a (1)-cell is an open interval $(a, b) \subseteq \mathbb{R}$.

(ii) Let $X \subseteq \mathbb{R}^n$ be a $(i_1, \ldots, i_n)$-cell and $f : X \to \mathbb{R}$ a continuous semi-algebraic function. Then $\{(\boldsymbol{x}, f(\boldsymbol{x})) \in \mathbb{R}^{n+1} : \boldsymbol{x} \in X\}$ is a $(i_1, \ldots, i_n, 0)$-cell, while $\{(\boldsymbol{x}, y) \in \mathbb{R}^{n+1} : \boldsymbol{x} \in X \wedge y < f(\boldsymbol{x})\}$ and $\{(\boldsymbol{x}, y) \in \mathbb{R}^{n+1} : \boldsymbol{x} \in X \wedge y > f(\boldsymbol{x})\}$ are both $(i_1, \ldots, i_n, 1)$-cells.

(iii) Let $X \subseteq \mathbb{R}^n$ be a $(i_1, \ldots, i_n)$-cell and $f, g : X \to \mathbb{R}$ continuous semi-algebraic functions such that $f(\boldsymbol{x}) < g(\boldsymbol{x})$ for all $\boldsymbol{x} \in X$. Then $\{(\boldsymbol{x}, y) \in \mathbb{R}^{n+1} : f(\boldsymbol{x}) < y < g(\boldsymbol{x})\}$ is a $(i_1, \ldots, i_n, 1)$-cell.

A cell in $\mathbb{R}^n$ is a $(i_1, \ldots, i_n)$-cell for some (necessarily unique) sequence $(i_1, \ldots, i_n)$.

A fundamental result about semi-algebraic sets, that we will use below, is the Cell-Decomposition Theorem [3]: given a semi-algebraic set $E \subseteq \mathbb{R}^n$ one can compute a partition of E as a disjoint of union of cells $E = C_1 \cup \ldots \cup C_m$.

We will also need the following result, proved in Appendix C.

▶ **Lemma 8.** *Let $D \subseteq \mathbb{R}^n$ be a semi-algebraic set, $g : D \to \mathbb{R}$ a bounded semi-algebraic function, and $r_1, \ldots, r_n$ real algebraic numbers. Define $S = \{t \in \mathbb{R}_{\geq 0} : (e^{r_1 t}, \ldots, e^{r_n t}) \in D\}$. Then*

(i) It is decidable whether or not S is bounded. If S is bounded then we can compute $T_0 \in \mathbb{N}$ such that $S \subseteq [0, T_0]$ and if S is unbounded then we can compute $T_0 \in \mathbb{N}$ such that $(T_0, \infty) \subseteq S$.

(ii) If S is unbounded then the limit $g^* = \lim_{t\to\infty} g(e^{r_1 t}, \ldots, e^{r_n t})$ exists, is an algebraic number, and there are effective constants $T_1, \varepsilon > 0$ such that $|g(e^{r_1 t}, \ldots, e^{r_n t}) - g^*| < e^{-\varepsilon t}$ for all $t > T_1$.

4.2 Two Linearly Independent Frequencies

The following lemma, which is a reformulation of [4, Lemma 13], plays an instrumental role in this section. The lemma itself relies on a powerful quantitative result in transcendence theory—Baker's Theorem on linear forms in logarithms of algebraic numbers [2].

▶ **Lemma 9.** *Let b_1, b_2 be real algebraic numbers, linearly independent over $\mathbb{Q}$. Furthermore, let φ_1, φ_2 be real numbers such that $e^{i\varphi_1}$ and $e^{i\varphi_2}$ are algebraic. Then there exist effectively computable constants $N, T > 0$ such that for all $t \geq T$ and all $k_1, k_2 \in \mathbb{Z}$, at least one of $|b_1 t - \varphi_1 - 2k_1\pi| > 1/t^N$ and $|b_2 t - \varphi_2 - 2k_2\pi| > 1/t^N$ holds.*

The main result of the section is the following.

▶ **Theorem 10.** *Let $f(t) = \sum_{j=1}^{n} e^{r_j t} (a_{1,j} \cos(\omega_j t) + a_{2,j} \sin(\omega_j t))$ be an exponential polynomial where $r_j, a_{1,j}, a_{2,j}, \omega_j$ are real algebraic numbers and the $\mathbb{Q}$-span of $\{\omega_1, \ldots, \omega_n\}$ has dimension two as a $\mathbb{Q}$-vector space. Then we can decide whether or not $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\}$ is bounded and, if bounded, we can compute an integer T such that $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\} \subseteq [0, T]$.*

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 9–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Proof. Let b_1, b_2 be real algebraic numbers, linearly independent over $\mathbb{Q}$, such that ω_j is an integer linear combination of b_1 and b_2 for $j = 1, \ldots, n$. For each $n \in \mathbb{Z}$, $\sin(nb_1t)$ and $\cos(nb_1t)$ can be written as polynomials in $\sin(b_1t)$ and $\cos(b_1t)$ with integer coefficients, and similarly for b_2. It follows that we can write f in the form

$$f(t) = Q(e^{r_1 t}, \ldots, e^{r_n t}, \cos(b_1 t), \sin(b_1 t), \cos(b_2 t), \sin(b_2 t))$$

for some polynomial Q with real algebraic coefficients that is computable from f.

Write $R_{++} = \{t \geq 0 : \sin(b_1t) \geq 0 \wedge \sin(b_2t) \geq 0\}$ and likewise define sets R_{+-}, R_{-+}, R_{--}, respectively corresponding to the other three sign conditions on $\sin(b_1t)$ and $\sin(b_2t)$. We show how to decide boundedness of $\{t \in R_{++} : f(t) = 0\}$. (The cases for R_{+-}, R_{-+}, and R_{--} follow *mutatis mutandis*.) The idea is to compute a partition of $\{t \in R_{++} : f(t) = 0\}$ into components $Z_1, \ldots, Z_m$ and to separately decide boundedness of each component Z_j.

Define a semi-algebraic set

$$E = \left\{(\boldsymbol{u}, x_1, x_2) \in \mathbb{R}^{n+2} : \exists y_1, y_2 \geq 0 \left(x_1^2 + y_1^2 = x_2^2 + y_2^2 = 1 \wedge Q(\boldsymbol{u}, x_1, y_1, x_2, y_2) = 0\right)\right\}.$$

Then for $t \in R_{++}$ we have $f(t) = 0$ if and only if $(e^{\boldsymbol{r}t}, \cos(b_1t), \cos(b_2t)) \in E$. Now consider a cell decomposition $E = C_1 \cup \ldots \cup C_m$ for cells $C_1, \ldots, C_m \subseteq \mathbb{R}^{n+2}$, and define

$$Z_j = \{t \in R_{++} : (e^{\boldsymbol{r}t}, \cos(b_1t), \cos(b_2t)) \in C_j\}, \qquad j = 1, \ldots, m, \tag{6}$$

Then $\{t \in R_{++} : f(t) = 0\} = Z_1 \cup \ldots \cup Z_m$.

Now fix $j \in \{1, \ldots, m\}$. We show how to decide boundedness of Z_j. To this end, write $D_j \subseteq \mathbb{R}^n$ for the projection of the corresponding cell $C_j \subseteq \mathbb{R}^{n+2}$ on the first n coordinates.

First suppose that $\{t \in \mathbb{R} : e^{\boldsymbol{r}t} \in D_j\}$ is bounded. Then by Proposition 8 we can compute an upper bound T of this set. But $Z_j \subseteq \{t \in \mathbb{R}_{\geq 0} : e^{\boldsymbol{r}t} \in D_j\}$ and so $Z_j \subseteq [0, T]$.

On the other hand, suppose that $\{t \in \mathbb{R} : e^{\boldsymbol{r}t} \in D_j\}$ is unbounded. Then, by Proposition 8, this set contains an unbounded interval (T, ∞) for some $T \in \mathbb{N}$. Write $I = [-1, 1]$ and define functions $g_1, g_2, h_1, h_2 : D_j \to \mathbb{R}$ by

$$g_1(\boldsymbol{u}) = \inf\{x \in I : \exists y\, (\boldsymbol{u}, x, y) \in C_j\} \qquad g_2(\boldsymbol{u}) = \inf\{y \in I : \exists x\, (\boldsymbol{u}, x, y) \in C_j\} \tag{7}$$

$$h_1(\boldsymbol{u}) = \sup\{x \in I : \exists y\, (\boldsymbol{u}, x, y) \in C_j\} \qquad h_2(\boldsymbol{u}) = \sup\{y \in I : \exists x\, (\boldsymbol{u}, x, y) \in C_j\} \tag{8}$$

These functions are all semi-algebraic by quantifier elimination. Hence by Lemma 8 the limits $g_i^* = \lim_{t\to\infty} g_i(e^{\boldsymbol{r}t})$ and $h_i^* = \lim_{t\to\infty} h_i(e^{\boldsymbol{r}t})$ exist for $i = 1, 2$ and are algebraic numbers. Clearly we have $g_1^* \leq h_1^*$ and $g_2^* \leq h_2^*$. We now consider three cases according to the strictness of these inequalities.

4.2.1 Case I: $g_1^* = h_1^*$ and $g_2^* = h_2^*$.

We show that Z_j is bounded and that we can compute T_2 such that $Z_j \subseteq [0, T_2]$.

By Lemma 8 there exist $T_1, \varepsilon > 0$ such that for all $t > T_1$ and $i = 1, 2$,

$$|g_i(e^{\boldsymbol{r}t}) - g_i^*| < e^{-\varepsilon t} \text{ and } |h_i(e^{\boldsymbol{r}t}) - h_i^*| < e^{-\varepsilon t}. \tag{9}$$

Then for $t \in R_{++}$ such that $t > T_1$ we have

$$\begin{aligned} t \in Z_j &\iff \left(e^{\boldsymbol{r}t}, \cos(b_1t), \cos(b_2t)\right) \in C_j \quad \text{(by (6))} \\ &\implies g_1(e^{\boldsymbol{r}t}) \leq \cos(b_1t) \leq h_1(e^{\boldsymbol{r}t}) \text{ and } g_2(e^{\boldsymbol{r}t}) \leq \cos(b_2t) \leq h_2(e^{\boldsymbol{r}t}) \quad \text{(by (8))} \\ &\implies |\cos(b_1t) - g_1^*| < e^{-\varepsilon t} \text{ and } |\cos(b_2t) - g_2^*| < e^{-\varepsilon t} \quad \text{(by (9))} \end{aligned} \tag{10}$$

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 10–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Write $g_1^* = \cos(\varphi_1)$ and $g_2^* = \cos(\varphi_2)$ for some $\varphi_1, \varphi_2 \in [0, \pi]$. Since $|\cos(\varphi_1 + x) - \cos(\varphi_1)| \geq x^3/3$ for all x sufficiently small (by a Taylor expansion), the inequality (10) implies that for some $k_1, k_2 \in \mathbb{Z}$,

$$|b_1 t - \varphi_1 - 2k_1\pi| < 3e^{-\varepsilon t/3} \text{ and } |b_2 t - \varphi_2 - 2k_2\pi| < 3e^{-\varepsilon t/3}\,. \tag{11}$$

Combining the upper bounds in (11) with the polynomial lower bounds $|b_1 t - \varphi_1 - 2k_1\pi| > 1/t^N$ and $|b_2 t - \varphi_2 - 2k_2\pi| > 1/t^N$ from Lemma 9 we obtain an effective bound T_2 for which $t \in Z_j$ implies $t < T_2$.

4.2.2 Case II: $g_1^* < h_1^*$.

In this case we show that Z_j is unbounded. The geometric intuition is as follows. We imagine a particle in the plane whose position at time t is $(\cos(b_1 t), \cos(b_2 t))$, together with a "moving target" whose extent at time t is $\Gamma_t = \{(x, y) : (e^{\boldsymbol{r}t}, x, y) \in C_j\}$. Below we essentially argue that such a particle is bound to hit Γ_t at some time t since its orbit is dense in $[-1, +1]^2$ and Γ_t has positive dimension in the limit.

Proceeding formally, first notice that C_j cannot be a $(\ldots, 0, 1)$-cell or a $(\ldots, 0, 0)$-cell, for then we would have $g_1(\boldsymbol{u}) = h_1(\boldsymbol{u})$ for all $\boldsymbol{u} \in D_j$ and hence $g_1^* = h_1^*$. Thus C_j must either be a $(\ldots, 1, 0)$-cell or a $(\ldots, 1, 1)$-cell. In either case, C_j includes a cell of the form $\{(\boldsymbol{u}, x, \xi(\boldsymbol{u}, x)) : \boldsymbol{u} \in D, g_1(\boldsymbol{u}) < x < h_1(\boldsymbol{u})\}$ for some semi-algebraic function ξ.

Let c, d be real algebraic numbers such that $g_1^* < c < d < h_1^*$. Write $c = \cos(\psi')$ and $d = \cos(\psi)$ for $0 \leq \psi < \psi' \leq \pi$. By Lemma 8 the limits $\lim_{t\to\infty} \xi(e^{\boldsymbol{r}t}, c)$ and $\lim_{t\to\infty} \xi(e^{\boldsymbol{r}t}, d)$ exist and are algebraic numbers in the interval $[-1, 1]$. Let $\theta, \theta' \in [0, \pi]$ be such that $\cos(\theta) = \lim_{t\to\infty} \xi(e^{\boldsymbol{r}t}, d)$ and $\cos(\theta') = \lim_{t\to\infty} \xi(e^{\boldsymbol{r}t}, c)$.

By Corollary 3 we know that $\frac{\theta'-\theta}{\psi'-\psi}$ is either rational or transcendental. In particular we know that it is not equal to $\frac{b_2}{b_1}$, which is algebraic and irrational. Let us suppose that $\frac{\theta'-\theta}{\psi'-\psi} > \frac{b_2}{b_1}$ (the converse case is almost identical). Then there exists θ'' with $\theta < \theta'' < \theta'$, such that

$$\theta < \theta'' + \frac{b_2}{b_1}(\psi' - \psi) < \theta'\,. \tag{12}$$

Since $2\pi, b_1, b_2$ are linearly independent over $\mathbb{Q}$ it follows from Kronecker's approximation theorem that $\{(b_1 t, b_2 t) \bmod 2\pi : t \in \mathbb{R}_{\geq 0}\}$ is dense in $[0, 2\pi)^2$ (see [12, Chapter 23]). Thus there is an increasing sequence $t_1 < t_2 < \ldots$, with $b_1 t_n \equiv \psi \bmod 2\pi$ for all n, such that $b_2 t_n \bmod 2\pi$ converges to θ''. Then, defining $s_1 < s_2 < \ldots$ by $s_n = t_n + \frac{\psi'-\psi}{b_1}$, we have $b_1 s_n \equiv \psi' \bmod 2\pi$ for all n and, by (12),

$$\lim_{n\to\infty} b_2 s_n = \lim_{n\to\infty} b_2 t_n + \frac{b_2}{b_1}(\psi' - \psi) = \theta'' + \frac{b_2}{b_1}(\psi' - \psi) < \theta' \pmod{2\pi}$$

Let $\eta(t) = \xi(e^{\boldsymbol{r}t}, \cos(b_1 t)) - \cos(b_2 t)$. Then for $t \in R_{++}$ such that $g(e^{\boldsymbol{r}t}) < \cos(b_1 t) < h(e^{\boldsymbol{r}t})$,

$$\begin{aligned} \eta(t) = 0 &\implies \cos(b_2 t) = \xi(e^{\boldsymbol{r}t}, \cos(b_1 t)) \\ &\implies (e^{\boldsymbol{r}t}, \cos(b_1 t), \cos(b_2 t)) \in C_j \\ &\implies t \in Z_j \text{ (by (6))}\,. \end{aligned}$$

Now $\lim_{n\to\infty} \eta(t_n) = \cos(\theta) - \cos(\theta'') > 0$ and $\lim_{n\to\infty} \eta(s_n) < \cos(\theta') - \cos(\theta') = 0$. Moreover for n sufficiently large we have $[t_n, s_n] \subseteq R_{++}$. It follows that $\eta(t)$ has a zero in every interval $[t_n, s_n]$ for n large enough. We conclude that Z_j is unbounded.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 11–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

4.2.3 Case III: $g_2^* < h_2^*$.

This case is symmetric to Case II and we omit details.

◀

References

1 Rajeev Alur. *Principles of Cyber-Physical Systems.* MIT Press, 2015.
2 Alan Baker. Transcendental number theory. 1975.
3 Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics).* Springer-Verlag, 2006.
4 Paul C. Bell, Jean-Charles Delvenne, Raphaël M. Jungers, and Vincent D. Blondel. The Continuous Skolem-Pisot Problem. *Theoretical Computer Science*, 411(40-42):3625–3634, 2010.
5 Richard P. Brent. Fast multiple-precision evaluation of elementary functions. *J. ACM*, 23(2):242–251, 1976.
6 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On recurrent reachability for continuous linear dynamical systems. Under review, 2016.
7 H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.
8 Paul M. Cohn. *Basic Algebra: Groups, Rings and Fields.* Springer, 2002.
9 David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, 2007.
10 Richard Guy. *Unsolved Problems in Number Theory.* Springer, third edition, 2004.
11 V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem's Problem – on the border between decidability and undecidability. Technical Report 683, Turku Centre for Computer Science, 2005.
12 GH Hardy and EM Wright. An introduction to the theory of numbers. *Oxford*, 1:979, 1999.
13 Eric Kaltofen. Polynomial factorization. In *(B. Buchberger, G. Collins, and R. Loos, editors) Computer Algebra*, pages 95–113. Springer, 1982.
14 Serge Lang. Introduction to transcendental numbers. *Reading, Mass*, 1966.
15 Angus Macintyre. Turing meets Schanuel. Preprint, to appear in the proceedings of Logic Colloquium 2012, 2015.
16 Angus Macintyre and Alex J Wilkie. On the decidability of the real exponential field. 1996.
17 V. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers and Mathematics with Applications*, 31(12):97 – 138, 1996.
18 Wolfgang Schmidt. Diophantine approximation. 785, 1980.
19 T. Tao. *Structure and randomness: pages from year one of a mathematical blog.* American Mathematical Society, 2008.
20 Kazuhiro Yokoyama, Masayuki Noro, and Taku Takeshima. Computing primitive elements of extension fields. *J. Symb. Comput.*, 8(6):553–580, 1989.
21 Boris Zilber. Exponential sums equations and the Schanuel conjecture. *Journal of the London Mathematical Society*, 65:27–44, 2002.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 12–19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

A One Linearly Independent Frequency

▶ **Theorem 11.** *Let* $f(t) = \sum_{j=1}^{n} e^{r_j t}\left(P_{1,j}(t)\cos(\omega_j t) + P_{2,j}\sin(\omega_j)\right)$ *be an exponential polynomial such that* $\omega_1, \ldots, \omega_n$ *are all integer multiples of single real algebraic number* b*. Then we can decide whether or not* $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\}$ *is bounded and, if bounded, we can compute an integer* T *such that* $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\} \subseteq [0, T]$*.*

Proof. Recall that for each integer n, both $\cos(nbt)$ and $\sin(nbt)$ can be written as polynomials in $\sin(bt)$ and $\cos(bt)$ with integer coefficients. It follows that we can write f in the form

$$f(t) = Q(t, e^{r_1 t}, \ldots, e^{r_n t}, \cos(bt), \sin(bt)),$$

for some multivariate polynomial Q with real algebraic coefficients that is computable from f.

Write $\mathbb{R}_{\geq 0}$ as the union of $R_+ := \{t \in \mathbb{R}_{\geq 0} : \sin(bt) \geq 0\}$ and $R_- := \{t \in \mathbb{R}_{\geq 0} : \sin(bt) \leq 0\}$. We show how to decide boundedness of $\{t \in R_+ : f(t) = 0\}$. The analogous case for R_- follows *mutatis mutandis*. The idea is to partition $\{t \in R_+ : f(t) = 0\}$ into components $Z_1, \ldots, Z_m$ and to show for how to decide boundedness of each Z_j.

To this end define a semi-algebraic set

$$E := \left\{(\boldsymbol{u}, x) \in \mathbb{R}^{n+2} : \exists y \geq 0 \left(x^2 + y^2 = 1 \wedge Q(\boldsymbol{u}, x, y) = 0\right)\right\}.$$

Then for all $t \in R_+$ we have $f(t) = 0$ if and only if $(t, e^{\boldsymbol{a}t}, \cos(bt)) \in E$.

Consider a cell decomposition $E = C_1 \cup \ldots \cup C_m$, for cells $C_1, \ldots, C_m \subseteq \mathbb{R}^{n+2}$, and define

$$Z_j = \{t \in R_+ : \left(t, e^{\boldsymbol{r}t}, \cos(bt)\right) \in C_j\}$$

for $j = 1, \ldots, m$. Then $\{t \in R_+ : f(t) = 0\} = Z_1 \cup \ldots \cup Z_m$.

We now focus on Z_j for some fixed $j \in \{1, \ldots, m\}$ and show how to decide whether or not Z_j is finite. Write $D_j \subseteq \mathbb{R}^{n+1}$ for the projection of the corresponding cell $C_j \subseteq \mathbb{R}^{n+2}$ onto the first $n+1$ coordinates. Then $Z_j \subseteq \{t \in \mathbb{R}_{\geq 0} : (t, e^{\boldsymbol{r}t}) \in D_j\}$.

First, suppose that $\{t \in \mathbb{R}_{\geq 0} : (t, e^{\boldsymbol{r}t}) \in D_j\}$ is bounded. Since D_j is semi-algebraic, by Proposition 18 we can compute an upper bound T of this set. In this case $t < T$ whenever $t \in Z_j$.

On the other hand, suppose that $\{t \in \mathbb{R} : (t, e^{\boldsymbol{r}t}) \in D_j\}$ is unbounded. Then, by Proposition 18, this set contains an unbounded interval (T, ∞). We claim that in this case Z_j must be unbounded. There are two cases according to the nature of the cell C_j.

A.0.3.1 Case I: C_j is a $(\ldots, 0)$-cell.

In this case there is a continuous semi-algebraic function $g : D_j \to \mathbb{R}$ such that $C_j = \{(\boldsymbol{u}, g(\boldsymbol{u})) : \boldsymbol{u} \in D_j\}$. Then for $t \in R_+ \cap (T, \infty)$,

$$\begin{aligned} g(t, e^{\boldsymbol{r}t}) = \cos(bt) &\iff (t, e^{\boldsymbol{r}t}, \cos(bt)) \in C_j \\ &\iff f(t) = 0\,. \end{aligned}$$

In other words, f has a zero at each point $t \in R_+ \cap (T, \infty)$ at which the graph of $g(t, e^{\boldsymbol{r}t})$ intersects the graph of $\cos(bt)$. Since g is a continuous function with an unbounded domain that takes values in $[-1, 1]$, there are infinitely many such intersection points–see Figure 1.

A.0.3.2 Case II: C_j is a $(\ldots, 1)$-cell.

In this case C_j contains some $(\ldots, 0)$-cell and so the argument in Case I shows that f has infinitely many zeros in Z_j. ◀

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 13–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

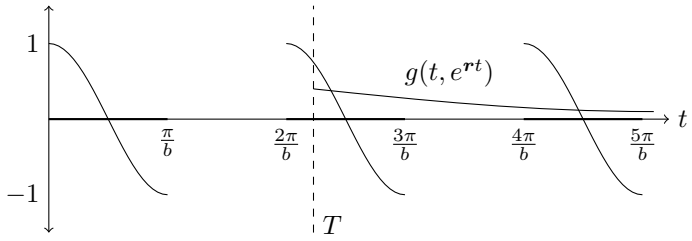

Figure 1 Intersection points of $g(t, e^{\boldsymbol{r}t})$ and $\cos(bt)$ for $t \in R_+$ (with R_+ shown in bold).

B Hardness

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 simple continued fraction expansion of a real number a is closely related to the *(homogeneous Diophantine approximation) type* of a, which is defined to be

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

Let $[n_1, n_2, n_3, \ldots]$ be the sequence of partial quotients in the simple continued fraction expansion of a. 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 simple 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 [10] 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 15, 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 15 is that in order to prove the decidability

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 14–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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:

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

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 12.** *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

$$t \geq 2\pi(m-1) \geq 2\pi m\alpha\,. \tag{13}$$

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 $|x| \leq \pi$:

$$\text{if } 1 - \cos(x) \leq c\pi/T \text{ then } \alpha x^2/2 \leq 1 - \cos(x). \tag{14}$$

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 (14) 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 (13), we have

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

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 15–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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

$$ce^{-t} \leq \left(\frac{c\varepsilon}{2a\alpha t}\right)^2 \quad \text{for } t \geq T. \tag{15}$$

Then the following chain of inequalities holds:

$$\begin{aligned}
\frac{\delta_1^2}{16} &\leq 1 - \cos(\delta_1) && \{ \text{ valid for all } |\delta_1| \leq \pi \ \} \\
&= \frac{c|\sin(\delta_2)| - t(1-\cos(\delta_2))}{e^t} && \{ \text{ since } f(t) = 0 \ \} \\
&\leq ce^{-t} && \{ \text{ since } |\sin(\delta_2)|, |\cos(\delta_2)| \leq 1 \} \\
&\leq \left(\frac{c\varepsilon}{2a\alpha t}\right)^2 && \{ \text{ by (15) } \} \\
&\leq \left(\frac{c\varepsilon}{4a\pi\alpha^2 m}\right)^2 && \{ \text{ by (13) } \}
\end{aligned}$$

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 13.** *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

$$\text{if } |x| < c(1-\varepsilon)/\pi M, \text{ then } (1-\varepsilon)|x| \leq |\sin(x)|. \tag{16}$$

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

$$\begin{aligned}
& f(t) \\
=\ & \{ \text{ as } \cos(t) = 1 \ \} \\
& t(1-\cos(\delta)) - c|\sin(\delta)| \\
\leq\ & \{ \text{ by (16) and } 1 - \cos(x) \leq x^2/2 \ \} \\
& \pi m\delta^2 - c(1-\varepsilon)|\delta| \\
\leq\ & \{ \text{ by } |\delta| \leq c(1-\varepsilon)/\pi m \ \} \\
& 0.
\end{aligned}$$

◀

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 16–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The following corollary is immediate:

▶ **Lemma 14.** *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 15.** *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 12 and 14. 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 12, $L(a) \leq B$ and we continue the approximation recursively on the interval $[p, B]$. If not, then $L(a) \geq A$ by Lemma 14, 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. ◀

We conclude by remarking that the exponential polynomials f_1 and f_2 involved in the proof of Theorem 15 involve only two rationally linearly independent frequencies. Thus the theorem applies as soon as we have a decision procedure for exponential polynomials with two rationally linear independent frequencies.

C Missing Proofs

C.1 Restatement and Proof of Proposition 1

▶ Proposition 16. 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 the form $P = \boldsymbol{z}^{\boldsymbol{u}}Q$ for some $Q \in \mathcal{R}$ with $Q = \overline{Q}$, 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 $P = Q + \boldsymbol{z}^{\boldsymbol{u}}\overline{Q}$.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 17–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

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. ◀

C.2 Restatement and Proof of Proposition 5

▶ Proposition 17. 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

$$P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) = 0 \tag{17}$$
$$Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) = 0 \tag{18}$$

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

Proof. Consider a solution $t \neq 0$ of Equations (17) and (18). 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 (17) and (18) still hold.

By Schanuel's conjecture, the extension

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

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

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

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

From Equations (17) and (18) 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., [9, 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 (17) and (18) have no non-zero solution $t \neq 0$. ◀

C.3 Restatement and Proof of Lemma 8

We divide Lemma 8 into two separate results, which are proven below.

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 18–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

▶ Proposition 18. There is a procedure that, given a semi-algebraic set $D \subseteq \mathbb{R}^{n+1}$ and real algebraic numbers $r_1, \ldots, r_n$, returns an integer T such that $\{t \geq 0 : (t, e^{r_1 t}, \ldots, e^{r_n t}) \in D\}$ either contains the interval (T, ∞) or is disjoint from (T, ∞). The procedure also decides which of these two eventualities is the case.

Proof. Consider a non-zero polynomial $P \in \mathbb{R}[x_0, \ldots, x_n]$ whose coefficients are real algebraic numbers. Then we can write $P(t, e^{r_1 t}, \ldots, e^{r_n t})$ in the form

$$Q_1(t)e^{\beta_1 t} + \ldots + Q_m(t)e^{\beta_m t}$$

for non-zero univariate polynomials $Q_1, \ldots, Q_m$ with real algebraic coefficients and real algebraic numbers $\beta_1 > \ldots > \beta_m$. It is clear that for t sufficiently large, $P(t, e^{r_1 t}, \ldots, a^{r_n t})$ has the same sign as the leading term $Q_1(t)$. The proposition easily follows. ◀

▶ **Lemma 19.** *Let $g : D \to \mathbb{R}$ be a bounded semi-algebraic function with domain $D \subseteq \mathbb{R}^n$. Let $\boldsymbol{r} = (r_1, \ldots, r_n)$ be a tuple of real algebraic numbers and T_1 an integer such that $e^{\boldsymbol{r}t} = (e^{r_1 t}, \ldots, e^{r_n t}) \in D$ for all $t > T_1$. Then the limit $g^* = \lim_{t\to\infty} g(e^{\boldsymbol{r}t})$ exists, is an algebraic number, and there are effective constants $T_2, \varepsilon > 0$ such that $|g(e^{\boldsymbol{r}t}) - g^*| < e^{-\varepsilon t}$ for all $t > T_2$.*

Proof. Since g is semi-algebraic, there is a non-zero polynomial P with real algebraic coefficients such that $P(\boldsymbol{x}, g(\boldsymbol{x})) = 0$ for all $\boldsymbol{x} \in D$ (see [3, Proposition 2.86]). In particular, we have $P(e^{\boldsymbol{r}t}, g(e^{\boldsymbol{r}t})) = 0$ for all $t > T_1$. Gathering terms, we can rewrite this equation in the form

$$Q_1(g(e^{\boldsymbol{r}t}))e^{\beta_1 t} + \ldots + Q_m(g(e^{\boldsymbol{r}t}))e^{\beta_m t} = 0$$

for non-zero univariate polynomials $Q_1, \ldots, Q_m$ with real-algebraic coefficients and real algebraic numbers $\beta_1 > \ldots > \beta_m$.

If $m = 1$ then for all $t > T_1$ we have $Q_1(g(e^{\boldsymbol{r}t})) = 0$. Thus $g(e^{\boldsymbol{r}t})$ is equal to some of root of Q for all $t > T_1$. Then by Proposition 18 there exists T_2 such that $g(e^{\boldsymbol{r}t}) = g^*$ for some fixed root g^* of Q_1 and all $t > T_2$.

If $m > 1$, since g is a bounded function, for all $t > T_1$ we have

$$\begin{aligned} \left|Q_1(g(e^{\boldsymbol{r}t}))\right| &= \left|Q_2(g(e^{\boldsymbol{r}t}))e^{(\beta_2-\beta_1)t} + \ldots + Q_m(g(e^{\boldsymbol{r}t}))e^{(\beta_m-\beta_1)t}\right| \\ &\leq Me^{(\beta_2-\beta_1)t} \end{aligned} \tag{19}$$

for some constant M. If Q_1 has degree d then (19) implies that the closest root of Q_1 to $g(e^{\boldsymbol{r}t})$ has distance at most $(Me^{\beta_2-\beta_1})^{1/d}$. Hence there exists a root g^* of Q_1 and effective constants $\varepsilon, T_2 > 0$ such that $|g(e^{\boldsymbol{r}t}) - g^*| < e^{-\varepsilon t}$ for all $t > T_2$. ◀

Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 19–19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany