



# On the Zeros of Exponential Polynomials

VENTSISLAV CHONEV, Max Planck Institute for Software Systems, Germany

JOEL OUAKNINE, Max Planck Institute for Software Systems, Germany

JAMES WORRELL, University of Oxford, United Kingdom

We consider the problem of deciding the existence of real roots of real-valued exponential polynomials with algebraic coefficients. Such functions arise as solutions of **linear differential equations with real algebraic coefficients**. We focus on two problems: the *Zero Problem*, which asks whether an exponential polynomial has a real root, and the *Infinite Zeros Problem*, which asks whether such a function has infinitely many real roots. Our main result is that for differential equations of order at most 8 the Zero Problem is decidable, subject to Schanuel's Conjecture, whilst the Infinite Zeros Problem is decidable unconditionally. We show moreover that a decision procedure for the Infinite Zeros Problem at order 9 would yield an algorithm for computing the Lagrange constant of any given real algebraic number to arbitrary precision, indicating that it will be very difficult to extend our decidability results to higher orders.

CCS Concepts: • **Computing methodologies** → **Symbolic and algebraic algorithms**; **Number theory algorithms**.

Additional Key Words and Phrases: linear differential equations, Diophantine approximation, Skolem problem, Baker's theorem, Schanuel Conjecture, semi-algebraic sets

## ACKNOWLEDGMENTS

Joël Ouaknine is also affiliated with Keble College, Oxford as emmy . network Fellow; he was supported by ERC grant AVS-ISS (648701) and by DFG grant 389792660 as part of TRR 248 (see <https://perspicuous-computing.science>). James Worrell is supported by UKRI Fellowship EP/X033813/1.

## 1 INTRODUCTION

This paper concerns root-finding problems for exponential polynomials, i.e., functions that satisfy ordinary linear differential equations with constant coefficients. The first problem we consider is the *Zero Problem*. This has as input an interval  $I \subseteq \mathbb{R}_{\geq 0}$  with rational (or infinite) endpoints and an ordinary differential equation

$$f^{(n)} + c_{n-1}f^{(n-1)} + \dots + c_0f = 0, \quad (1)$$

with the coefficients  $c_0, \dots, c_{n-1}$  and initial conditions  $f(0), \dots, f^{(n-1)}(0)$  being real algebraic numbers. Writing  $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$  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 the Zero Problem is currently open. Indeed decidability is open even for the version of the problem in which we only allow bounded intervals  $I$ , called the *Bounded Zero Problem* [2, Open Problem 17]. We also study the *Infinite Zeros Problem*, which asks whether  $f$  has infinitely many zeros over the nonnegative reals.

We recall some terminology in order to state our main contributions. Every solution of (1) has the form  $f(t) = \sum_{j=1}^m P_j(t)e^{\lambda_j t}$ , where  $\lambda_1, \dots, \lambda_m$  are the characteristic roots of the differential equation and  $P_1, \dots, P_m$  are

---

Authors' addresses: VENTSISLAV CHONEV, Max Planck Institute for Software Systems, Saarbrücken, Germany, [v.chonev@gmail.com](mailto:v.chonev@gmail.com); JOEL OUAKNINE, Max Planck Institute for Software Systems, Saarbrücken, Germany, [joel@mpi-sws.org](mailto:joel@mpi-sws.org); JAMES WORRELL, Department of Computer Science, University of Oxford, Oxford, United Kingdom, [jbw@cs.ox.ac.uk](mailto:jbw@cs.ox.ac.uk).

---

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2023 Copyright held by the owner/author(s).

0004-5411/2023/6-ART

<https://doi.org/10.1145/3603543>

polynomials that are determined by the initial conditions. We call  $f$  an *exponential polynomial*. The *frequencies* of  $f$  are the imaginary parts of the characteristic roots and the polynomials  $P_j$  are called the *coefficients* of  $f$ . The *order* of  $f$  is the least number  $n$  such that  $f$  satisfies a differential equation of the form (1).

Our first main result establishes decidability of the Bounded Zero Problem subject to Schanuel's Conjecture, a unifying conjecture in transcendental number theory that plays a key role in the study of the exponential function over both the real and complex numbers [21, 22]. We use Schanuel's Conjecture to show that every exponential polynomial admits a factorisation such that the zeros of each factor are simple and can be detected using finite-precision numerical computations.

A celebrated paper of Macintyre and Wilkie [18] obtains decidability of the first-order theory of the structure  $\mathfrak{R}_{\text{exp}} = (\mathbb{R}, 0, 1, <, \cdot, +, \exp)$  assuming Schanuel's Conjecture over  $\mathbb{R}$ . The proof of [17, Theorem 3.1] refers to unpublished work of Macintyre and Wilkie that extends the above-mentioned result to obtain decidability when  $\mathfrak{R}_{\text{exp}}$  is augmented with the restricted functions  $\sin \upharpoonright_{[0, 2\pi]}$  and  $\cos \upharpoonright_{[0, 2\pi]}$ , this time assuming Schanuel's Conjecture over  $\mathbb{C}$ . This result immediately implies decidability of the Bounded Zero Problem. However, decidability of the latter problem is much simpler and, as we show in Section 3, can be established by a direct application of Schanuel's Conjecture.

Our second main result, spanning Sections 4 and 5, shows that the Infinite Zeros Problem is decidable for the class of exponential polynomials of order at most 8. We show moreover that if such a function has finitely many zeros then an upper bound on the magnitude of the largest zero can be computed. We thereby reduce the Zero Problem to the Bounded Zero Problem, and obtain decidability of the former up to order 8, conditional on Schanuel's Conjecture. Decidability of the Infinite Zeros Problem is unconditional and relies on various results in real-algebraic geometry, transcendental number theory and Diophantine approximation, such as the cell decomposition theorem for semi-algebraic sets, Baker's theorem on linear forms in logarithms of algebraic numbers, and Kronecker's simultaneous approximation theorem.

We complete the picture in Section 6 by showing that decidability of the Infinite Zeros Problem at order 9 would entail a major new effectiveness result in Diophantine approximation—namely computability of the Lagrange constants of all real algebraic numbers. As discussed below, currently essentially nothing is known about the Lagrange constants of algebraic numbers of degree three or higher and there are several longstanding open problems connected to this question. Thus, the exhibited reduction represents a significant barrier to extending the positive decidability results in this paper. An analogous hardness result can be proven for the Zero Problem [6, Chapter 6.4].

## 1.1 Related work

To the best of our knowledge the Zero Problem and Infinite Zeros Problem were first studied in [2]. That work established decidability of the Infinite Zeros problem in the special case the dominant characteristic roots are simple, are at least four in number, and have imaginary parts linearly independent over  $\mathbb{Q}$  (see [2, Theorem 15]).

The Zero Problem can be seen as a continuous analog of Skolem's Problem for linear recurrence sequences, which asks whether a given linear recurrence sequence has a zero term [11]. Decidability of Skolem's Problem is known for recurrences of order at most four but is open in general. Likewise the Infinite Zeros Problem can be seen as a continuous analog of the problem of whether a given linear recurrence sequence has infinitely many zero terms. Decidability of the latter problem was established in [3].

## 2 PRELIMINARIES

### 2.1 Exponential polynomials

Consider a homogeneous linear differential equation

$$f^{(n)} + c_{n-1}f^{(n-1)} + \dots + c_0f = 0 \quad (2)$$

of order  $n$  with complex coefficients  $c_0, \dots, c_{n-1}$ . The *characteristic polynomial* of (2) is

$$\chi(x) := x^n + c_{n-1}x^{n-1} + \dots + c_0. \quad (3)$$

Given initial values of  $f(0), f'(0), \dots, f^{(n-1)}(0)$ , the uniquely defined solution  $f$  of (2) can be expressed as an *exponential polynomial*  $f(t) = \sum_{j=1}^k P_j(t)e^{\lambda_j t}$ , where  $\lambda_1, \dots, \lambda_k$  are the distinct roots of  $\chi$  and for all  $j$ ,  $P_j$  is a polynomial of degree one less than the multiplicity of  $\lambda_j$  as a root of  $\chi$ . In particular, if the roots of  $\chi$  are all simple then  $f$  has constant coefficients. We call the polynomials  $P_j$  the *coefficients* of  $f$  and we call the numbers  $\lambda_j$  the *exponents* of  $f$ . We refer to the exponents with maximum real part as *dominant*.

If the coefficients of the differential equation (2) and the initial values of the derivatives of  $f$  are all real algebraic then the exponents and their corresponding coefficients come in complex-conjugate pairs, and  $f$  has the form

$$f(t) = \sum_{j=1}^k e^{a_j t} \sum_{l=0}^{m_j-1} C_{j,l} t^l \cos(b_j t + \varphi_{j,l}) \quad (4)$$

where the  $a_j, b_j, C_{j,l}$  are real algebraic and the  $\varphi_{j,l}$  are real numbers such that  $e^{i\varphi_{j,l}}$  is algebraic for all  $j, l$ . Both solution forms (3) and (4) can be computed from the differential equation and initial conditions. We refer the reader to [2, Theorem 7] for details.

Unless explicitly specified otherwise, throughout this paper exponential polynomials are assumed to be real-valued; however complex-valued ones arise in Section 3.

### 2.2 Computational algebraic number theory

We denote by  $\overline{\mathbb{Q}}$  the set of algebraic numbers. For computational purposes we assume a representation of algebraic numbers (such as that described in [7, Section 4.2.1]) that allows to effectively perform arithmetic and to compute the roots of polynomials with algebraic coefficients.

Given an exponential polynomial  $f = \sum_{j=1}^m P_j(t)e^{\lambda_j t}$ , consider the field  $K = \mathbb{Q}(\lambda_1, \dots, \lambda_m)$ . Note that  $K$  is closed under complex conjugation. We can compute a primitive element of  $K$ , that is, an algebraic number  $\theta$  such that  $K = \mathbb{Q}(\theta)$ , together with a representation of each  $\lambda_j$  as a polynomial in  $\theta$  with rational coefficients (see [7, Section 4.5]). From the representation of  $\lambda_1, \dots, \lambda_m$  as elements of  $\mathbb{Q}(\theta)$ , it is straightforward to determine maximal  $\mathbb{Q}$ -linearly independent subsets of  $\{\operatorname{Re}(\lambda_j) : 1 \leq j \leq m\}$  and  $\{\operatorname{Im}(\lambda_j) : 1 \leq j \leq m\}$  (see [13, Section 1]).

### 2.3 Transcendental number theory

We will need the following two classical results from transcendental number theory [14].

**THEOREM 2.1 (GELFOND-SCHNEIDER).** *If  $a, b \in \overline{\mathbb{Q}}$  with  $a \neq 0, 1$  and  $b \notin \mathbb{Q}$ , then  $a^b$  is transcendental.*

**THEOREM 2.2 (LINDEMANN-WEIERSTRASS).** *If  $a_1, \dots, a_n \in \overline{\mathbb{Q}}$  are linearly independent over  $\mathbb{Q}$ , then  $e^{a_1}, \dots, e^{a_n}$  are algebraically independent over  $\mathbb{Q}$ .*

An easy consequence of the Lindemann-Weierstrass Theorem is that a non-zero algebraic root  $\alpha$  of an exponential polynomial  $f(t) = \sum_{j=1}^k P_j(t)e^{\lambda_j t}$  satisfies  $P_1(\alpha) = \dots = P_k(\alpha) = 0$ .

The following lemma, proven in [2], is a consequence of Baker's theorem on linear forms in logarithms of algebraic numbers.

LEMMA 2.3. [2, Lemma 13] Let  $a, b \in \mathbb{R} \cap \overline{\mathbb{Q}}$  be linearly independent over  $\mathbb{Q}$  and let  $i\varphi_1, i\varphi_2$  be logarithms of algebraic numbers, that is,  $e^{i\varphi_1}, e^{i\varphi_2} \in \overline{\mathbb{Q}}$ . There exist effective constants  $C, N, T > 0$  such that for all  $t \geq T$ , at least one of  $1 - \cos(at + \varphi_1) > C/t^N$  and  $1 - \cos(bt + \varphi_2) > C/t^N$  holds.

Our results on the Bounded Zero Problem depend on Schanuel's Conjecture, a unifying conjecture in transcendental number theory [14], whose statement generalises many of the central results in the field (including Theorems 2.1 and 2.2). 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 2.4 (SCHANUEL'S CONJECTURE, SEE [14]). Let  $a_1, \dots, a_n$  be complex numbers that are linearly independent over  $\mathbb{Q}$ . Then the field  $\mathbb{Q}(a_1, \dots, a_n, e^{a_1}, \dots, e^{a_n})$  has transcendence degree at least  $n$  over  $\mathbb{Q}$ .

## 2.4 Diophantine approximation

Another key tool is a version of Kronecker's theorem in Diophantine approximation.

THEOREM 2.5. (Kronecker, see [5, Chap. 7, Sec. 1.3, Prop. 1.7]) Let  $\lambda_1, \dots, \lambda_m$  and  $x_1, \dots, x_m$  be real numbers. Suppose that for all integers  $u_1, \dots, u_m$  such that  $u_1\lambda_1 + \dots + u_m\lambda_m \in \mathbb{Z}$ , we also have  $u_1x_1 + \dots + u_mx_m \in \mathbb{Z}$ . Then for all  $\varepsilon > 0$ , there exist  $p \in \mathbb{Z}^m$  and  $n \in \mathbb{N}$  such that  $|n\lambda_j - x_j - p_j| < \varepsilon$  for all  $1 \leq j \leq m$ . In particular, if  $1, \lambda_1, \dots, \lambda_m$  are linearly independent over  $\mathbb{Z}$ , then for all  $x \in \mathbb{R}^m$  and  $\varepsilon > 0$  there exist  $n \in \mathbb{N}$  and  $p \in \mathbb{Z}^m$  such that  $|n\lambda_j - x_j - p_j| < \varepsilon$ .

A direct consequence is the following:

PROPOSITION 2.6. Let  $a_1, \dots, a_m \in \mathbb{R} \cap \overline{\mathbb{Q}}$  be linearly independent over  $\mathbb{Q}$  and let  $\varphi_1, \dots, \varphi_m \in \mathbb{R}$ . Given  $x \in \mathbb{R}$ , denote by  $x \bmod 2\pi$  the unique value  $x' \in [0, 2\pi)$  such that  $x - x' \in 2\pi\mathbb{Z}$ . Then the image of the mapping  $h(t) : \mathbb{R}_{\geq 0} \rightarrow [0, 2\pi)^m$  given by

$$h(t) = ((a_1t + \varphi_1) \bmod 2\pi, \dots, (a_mt + \varphi_m) \bmod 2\pi)$$

is dense in  $[0, 2\pi)^m$ . Moreover, the set

$$\{h(t) \mid (a_1t + \varphi_1) \bmod 2\pi = 0\}$$

is dense in  $\{0\} \times [0, 2\pi)^{m-1}$ .

PROOF. For the first part of the claim, it is clear that  $1, a_1/2\pi, \dots, a_m/2\pi$  are rationally linearly independent and hence, by Kronecker's Theorem (Theorem 2.5), the set  $\{h(t) \mid t \in \mathbb{N}\}$  is dense in  $[0, 2\pi)^m$ . It follows that  $\{h(t) \mid t \in \mathbb{R}_{\geq 0}\}$  is also dense in  $[0, 2\pi)^m$ . For the second part, note that the first coordinate of  $h(t)$  is zero precisely when  $t = -\varphi_1/a_1 + 2n\pi$  for some  $n \in \mathbb{Z}$ . At such a time we have  $h(t) = (0, g(n))$ , where

$$g(n) \stackrel{\text{def}}{=} \left\langle \left( n \frac{2\pi a_j}{a_1} + \frac{a_1 \varphi_j - \varphi_1 a_j}{a_1} \right) \bmod 2\pi : 2 \leq j \leq m \right\rangle.$$

As above, we have that  $\{1, 2\pi a_2/a_1, \dots, 2\pi a_m/a_1\}$  are linearly independent over  $\mathbb{Q}$ , so applying Kronecker's Theorem (Theorem 2.5), we have that  $\{g(n) : n \in \mathbb{N}\}$  is dense in  $[0, 2\pi)^m$ .  $\square$

We will also need the following quantitative version of the one-dimensional case of Kronecker's Theorem.

THEOREM 2.7. (Chebyshev, see [12, Theorem 440]) If  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  and  $\beta \in \mathbb{R}$ , then there are infinitely many pairs of integers  $l, k$  with  $k > 0$  such that  $k|\alpha k + l + \beta| < 2$ .

## 2.5 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  $P(x_1, \dots, x_n) > 0$ , where  $P$  is a polynomial with real algebraic coefficients. A partial function  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  is semi-algebraic if its graph is a semi-algebraic subset of  $\mathbb{R}^{n+1}$ . The Tarski-Seidenberg theorem [4, Section 1] 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  $(i_1, \dots, i_n)$  be a sequence of zeros and ones of length  $n \geq 1$ . An  $(i_1, \dots, i_n)$ -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  $(i_1, \dots, i_n)$ -cell and  $f : X \rightarrow \mathbb{R}$  a continuous semi-algebraic function. Then  $\{(x, f(x)) \in \mathbb{R}^{n+1} : x \in X\}$  is a  $(i_1, \dots, i_n, 0)$ -cell, while  $\{(x, y) \in \mathbb{R}^{n+1} : x \in X \wedge y < f(x)\}$  and  $\{(x, y) \in \mathbb{R}^{n+1} : x \in X \wedge y > f(x)\}$  are both  $(i_1, \dots, i_n, 1)$ -cells.
- (iii) Let  $X \subseteq \mathbb{R}^n$  be a  $(i_1, \dots, i_n)$ -cell and  $f, g : X \rightarrow \mathbb{R}$  continuous semi-algebraic functions such that  $f(x) < g(x)$  for all  $x \in X$ . Then  $\{(x, y) \in \mathbb{R}^{n+1} : f(x) < y < g(x)\}$  is a  $(i_1, \dots, i_n, 1)$ -cell.

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

The following is a fundamental result about semi-algebraic sets [1, 19]:

**THEOREM 2.8. (Cell decomposition theorem)** *Given a semi-algebraic set  $E \subseteq \mathbb{R}^n$ , one can compute a partition of  $E$  as a disjoint union of cells  $E = C_1 \cup \dots \cup C_m$ .*

We will need the following two simple results about the real exponential function.

**PROPOSITION 2.9.** *There is a procedure which, given a semi-algebraic set  $D \subseteq \mathbb{R}^{n+1}$  and real algebraic numbers  $r_1, \dots, r_n$ , decides whether the set  $S = \{t \geq 0 : (t, e^{r_1 t}, \dots, e^{r_n t}) \in D\}$  is bounded, and moreover returns an integer  $T$ , such that if  $S$  is bounded, then  $S \subseteq [0, T]$ , and if  $S$  is unbounded, then  $(T, \infty) \subseteq S$ .*

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

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

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

**PROPOSITION 2.10.** *Let  $g : D \rightarrow \mathbb{R}$  be a bounded semi-algebraic function with domain  $D \subseteq \mathbb{R}^n$ . Let  $\mathbf{r} = (r_1, \dots, r_n)$  be a tuple of real algebraic numbers and  $T_1$  an integer such that  $e^{\mathbf{r}t} = (e^{r_1 t}, \dots, e^{r_n t}) \in D$  for all  $t > T_1$ . Then the limit  $g^* = \lim_{t \rightarrow \infty} g(e^{\mathbf{r}t})$  exists, is an algebraic number, and there are effective constants  $T_2, \varepsilon > 0$  such that  $|g(e^{\mathbf{r}t}) - g^*| < e^{-\varepsilon t}$  for all  $t > T_2$ .*

**PROOF.** Since  $g$  is semi-algebraic, there is a non-zero polynomial  $P$  with real algebraic coefficients such that  $P(x, g(x)) = 0$  for all  $x \in D$  (see [1, Proposition 2.86]). In particular, we have  $P(e^{\mathbf{r}t}, g(e^{\mathbf{r}t})) = 0$  for all  $t > T_1$ . Gathering terms, we can rewrite this equation in the form

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

for non-zero univariate polynomials  $Q_1, \dots, Q_m$  with real-algebraic coefficients and real algebraic numbers  $\beta_1 > \dots > \beta_m$ . Without loss of generality, assume that  $Q_1$  is monic.

If  $m = 1$  then for all  $t > T_1$  we have  $Q_1(g(e^{\mathbf{r}t})) = 0$ . Thus  $g(e^{\mathbf{r}t})$  is equal to some root of  $Q_1$  for all  $t > T_1$ . Then by Proposition 2.9 there exists  $T_2$  and a root  $g^*$  of  $Q_1$  such that  $g(e^{\mathbf{r}t}) = g^*$  for all  $t > T_2$ .

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

$$|Q_1(g(e^{rt}))| = |Q_2(g(e^{rt}))e^{(\beta_2-\beta_1)t} + \dots + Q_m(g(e^{rt}))e^{(\beta_m-\beta_1)t}| \leq Me^{(\beta_2-\beta_1)t} \quad (5)$$

for some constant  $M$ . Let  $Q_1$  have degree  $d$ . Since  $Q_1$  is monic, (5) implies that the distance of  $g(e^{rt})$  to a root of  $Q_1$  is at most  $(Me^{(\beta_2-\beta_1)t})^{1/d}$ . Hence there exists a root  $g^*$  of  $Q_1$  and effective constants  $\varepsilon, T_2 > 0$  such that  $|g(e^{rt}) - g^*| < e^{-\varepsilon t}$  for all  $t > T_2$ .  $\square$

### 3 BOUNDED ZERO PROBLEM

In this section we show that the Bounded Zero Problem is decidable. Recall that in this problem we are given a real-valued exponential polynomial  $f$  and a bounded interval  $I$ , and we wish to determine whether  $f(t) = 0$  for some  $t \in I$ . A natural approach is to apply numerical zero-finding techniques. The main obstacle here is to bound the required precision, e.g., consider how one might determine numerically whether a local minimum of  $f$  is a zero. To circumvent this obstacle, we first write  $f$  as a product of irreducible factors, working over a certain ring of *Laurent polynomials*, and study the zeros of the factors separately. This factorisation allows us to discount repeated real zeros (assuming Schanuel's Conjecture). Note that the factors of a given real-valued exponential polynomial may be complex-valued.

#### 3.1 Zero finding

In this section we describe a method for deciding whether an exponential polynomial  $f : \mathbb{C} \rightarrow \mathbb{C}$  has a zero in a given bounded open interval  $(a, b)$  in the real line. The idea is to cover the interval  $(a, b)$  by disks in the complex plane and determine the number of zeros of  $f$  in each disk using the argument principle in complex analysis. Such an approach underlies several root-finding algorithms for polynomials (see, e.g., [15]); however in the absence of root separation bounds for exponential polynomials, we require additional assumptions on  $f$  in order to distinguish real from imaginary roots. Establishing these conditions ultimately relies on Schanuel's Conjecture.

Recall the following classical theorem of complex analysis:

**THEOREM 3.1 (ARGUMENT PRINCIPLE).** *Let  $f : \mathbb{C} \rightarrow \mathbb{C}$  be a holomorphic function and  $C$  a positively oriented simple closed contour in  $\mathbb{C}$  on which  $f$  has no zeros. Then*

$$\oint_C \frac{f'(z)}{f(z)} dz = 2\pi i N, \quad (6)$$

where  $N$  denotes the number of zeros of  $f$  in the region enclosed by  $C$ , where each zero is counted as many times as its multiplicity.

We briefly explain how to evaluate integrals of the form (6) in case  $f$  is an exponential polynomial and  $C$  is a circular contour that does not contain a root of  $f$ . We assume that  $f$  has algebraic coefficients, and  $C$  has centre  $p + qi$  and radius  $r$  for some  $p, q, r \in \mathbb{Q}$ . Consider the parametrisation  $\gamma : [0, 1] \rightarrow \mathbb{C}$  of  $C$  given by  $\gamma(t) = p + qi + re^{2\pi i t}$ . Then the integral (6) can be written in the form  $\int_0^1 g(t) dt$  for the function

$$g(t) = \frac{f'(\gamma(t))\gamma'(t)}{f(\gamma(t))}.$$

Now it is straightforward to compute a constant  $L_1 > 0$  such that  $f \circ \gamma$  is  $L_1$ -Lipschitz. By approximating the value of  $f$  at sufficiently many values on  $C$  one can compute  $\varepsilon > 0$  such that  $|f(z)| > \varepsilon$  for all  $z \in C$ . Using this lower bound we can in turn compute a constant  $L_2 > 0$  such that the function  $g(t)$  is  $L_2$ -Lipschitz. It follows that

INPUT: Exponential polynomial  $f$  and  $a, b \in \mathbb{Q}$ .

OUTPUT: Whether  $f$  has a real root in the interval  $(a, b)$ .

For  $k \in \{1, 2, 3, \dots\}$  do

- (1) Cover the line segment  $(a, b)$  by  $k$  equally sized circular contours  $C_1, \dots, C_k$ , where for all  $j \in \{1, \dots, k\}$  circle  $C_j$  has centre  $a + (b - a)\frac{2j-1}{2k}$  and radius  $\frac{b-a}{2k}$ .
- (2) For  $j \in \{1, \dots, k\}$ , compute a strictly positive lower bound for  $|f|$  on  $C_j$  and compute the number  $N_j$  of complex zeros of  $f$  on the region enclosed by  $C_j$ .
- (3) If  $N_j$  is odd for some  $j \in \{1, \dots, k\}$  then halt and return that  $f$  has a zero on  $[a, b]$ .
- (4) If  $N_j = 0$  for all  $j \in \{1, \dots, k\}$  then halt and return that  $f$  has no zero on  $[a, b]$ .

Fig. 1. Root-finding procedure for exponential polynomials

for all  $n > 0$ ,

$$\left| \int_0^1 g(t) dt - \frac{1}{n} \sum_{k=1}^n g\left(\frac{k}{n}\right) \right| \leq \frac{L_2}{n}.$$

Thus we can approximate the integral in (6) to arbitrary precision and thereby determine  $N$ .

**PROPOSITION 3.2.** *Let  $f : \mathbb{C} \rightarrow \mathbb{C}$  be an exponential polynomial with algebraic coefficients and exponents. Assume that all real zeros of  $f$  are simple and that complex zeros of  $f$  come in complex-conjugate pairs (i.e., for all  $z \in \mathbb{C}$ ,  $f(z) = 0$  iff  $f(\bar{z}) = 0$ ). Then we can decide whether  $f$  has a zero in a given open interval  $(a, b)$  with rational endpoints.*

**PROOF.** We argue that the procedure in Figure 1 determines whether  $f$  has a zero in the interval  $(a, b)$ .

If the procedure terminates in Line (4) then the output is correct by a direct application of Theorem 3.1. If the procedure terminates in Line (3) then the output is correct by the assumption that the real roots of  $f$  are simple and complex roots come in conjugate pairs; in conjunction with Theorem 3.1 this entails that  $N_j$  is odd just in case  $C_j$  contains a real root. It remains to argue that the procedure always terminates.

For a given value of  $k$ , Line (2) succeeds if  $f$  has no zero on any of the contours  $C_j$ . Since  $f$  has only finitely many zeros in any bounded region of the complex plane, for  $k$  sufficiently large the body of the for loop will terminate. Moreover for  $k$  sufficiently large, each contour  $C_j$  will enclose at most one real root and no complex roots and thus the whole procedure will halt. Thus termination is assured if we evaluate the loop for all values of  $k$  in parallel in a fair way (e.g., divide the computation into phases such that in the  $m$ -th phase one executes  $m$  steps of the loop body for  $k = 1, \dots, m$ ).  $\square$

### 3.2 Laurent polynomials

Fix non-negative integers  $r$  and  $s$ , and consider a single variable  $X$  and tuples of variables  $Y = \langle Y_1, \dots, Y_r \rangle$  and  $Z = \langle Z_1, \dots, Z_s \rangle$ . Consider the ring of Laurent polynomials

$$\mathcal{R} := \mathbb{C}[X, Y_1, Y_1^{-1}, \dots, Y_r, Y_r^{-1}, Z_1, Z_1^{-1}, \dots, Z_s, Z_s^{-1}],$$

which can be seen as a localisation of the polynomial ring

$$\mathcal{A} := \mathbb{C}[X, Y_1, \dots, Y_r, Z_1, \dots, Z_s]$$

in the set of monomials in variables  $Y_1, \dots, Y_r$  and  $Z_1, \dots, Z_s$ . The multiplicative units of  $\mathcal{R}$  are the non-zero monomials in variables  $Y_1, \dots, Y_r$  and  $Z_1, \dots, Z_s$ . As the localisation 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 irreducible polynomials that also have algebraic coefficients and that this factorisation can be effectively computed [16].

We define an involution on  $\mathcal{R}$  (that is, a self-inverse ring automorphism) as follows. Given a polynomial

$$P(X, Y, Z) = \sum_{j=1}^n \alpha_j X^{u_j} Y_1^{v_{j,1}} \dots Y_r^{v_{j,r}} Z_1^{w_{j,1}} \dots Z_s^{w_{j,s}},$$

where  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ , define

$$P^*(X, Y, Z) := \sum_{j=1}^n \overline{\alpha_j} X^{u_j} Y_1^{v_{j,1}} \dots Y_r^{v_{j,r}} Z_1^{-w_{j,1}} \dots Z_s^{-w_{j,s}}.$$

As we will see shortly, the mapping  $(-)^*$  on  $\mathcal{R}$  corresponds to a natural operation on exponential polynomials.

Consider an exponential polynomial  $f : \mathbb{C} \rightarrow \mathbb{C}$  given by

$$f(z) := \sum_{j=1}^n P_j(z) e^{\lambda_j z},$$

where  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  are algebraic numbers and  $P_1, \dots, P_n \in \mathbb{C}[z]$  are univariate polynomials with algebraic coefficients. Let  $\{a_1, \dots, a_r\}$  be a basis of the  $\mathbb{Q}$ -vector space spanned by  $\{\operatorname{Re}(\lambda_j) : 1 \leq j \leq n\}$  and let  $\{b_1, \dots, b_s\}$  be a basis of the  $\mathbb{Q}$ -vector space spanned by  $\{\operatorname{Im}(\lambda_j) : 1 \leq j \leq n\}$ . Without loss of generality we may assume that each characteristic root  $\lambda$  is an integer linear combination of  $a_1, \dots, a_r$  and  $ib_1, \dots, ib_s$ . Then  $e^{\lambda z}$  is a product of positive and negative powers of  $e^{a_1 z}, \dots, e^{a_r z}$  and  $e^{ib_1 z}, \dots, e^{ib_s z}$ . It follows that there is a Laurent polynomial  $P \in \mathcal{R}$  such that

$$f(z) = P(z, e^{a_1 z}, \dots, e^{a_r z}, e^{ib_1 z}, \dots, e^{ib_s z}). \quad (7)$$

Given the exponential polynomial  $f$  in (7) we are led to define  $f^* : \mathbb{C} \rightarrow \mathbb{C}$  by

$$f^*(z) := P^*(z, e^{a_1 z}, \dots, e^{a_r z}, e^{ib_1 z}, \dots, e^{ib_s z}).$$

Clearly  $f^*$  is an exponential polynomial and, by definition of  $P^*$ , we have  $f^*(z) = \overline{f(\bar{z})}$  for all  $z \in \mathbb{C}$ .

Since the polynomial  $P$  in (7) can be written as a product of irreducible factors in the ring of Laurent polynomials  $\mathcal{R}$ , the exponential polynomial  $f$  can be written as product of exponential polynomials of the form

$$g(z) = Q(z, e^{a_1 z}, \dots, e^{a_r z}, e^{ib_1 z}, \dots, e^{ib_s z}) \quad (8)$$

with  $Q \in \mathcal{R}$  irreducible. We now classify such exponential polynomials into two types.

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  $g$  in (8). We say that  $g$  is a *Type-1 exponential polynomial* if  $Q$  is irreducible and if  $Q$  and  $Q^*$  are not associates in  $\mathcal{R}$  (i.e.  $Q$  is not the product of  $Q^*$  with a monomial in  $Y_1, \dots, Y_r, Z_1, \dots, Z_s$ ). We say that  $g$  is a *Type-2 exponential polynomial* if  $Q$  is irreducible and if  $Q$  and  $Q^*$  are associates in  $\mathcal{R}$ .

*Example 3.3.* A simple example of a Type-2 exponential polynomial is  $g(z) = 1 + e^{iz}$ . Here  $g(z) = Q(e^{iz})$ , where  $Q(Z) = 1 + Z$  is an irreducible polynomial that is associated with its conjugate  $Q^*(Z) = 1 + Z^{-1}$  (since  $Q = ZQ^*$ ).

### 3.3 Conditional decidability

In this section we present a decision procedure for the Bounded Zero Problem.

Since the ring  $\mathcal{R}$  has factorisation into irreducibles, an arbitrary exponential polynomial can be written as a product of Type-1 and Type-2 exponential polynomials. Moreover, as noted above, this factorisation can be computed from  $f$ . Thus it suffices to show how to decide the existence of zeros of Type-1 and Type-2 exponential polynomials. We will handle both cases using Schanuel's conjecture via the following proposition.



PROPOSITION 3.4. *Given non-negative integers  $r$  and  $s$ , let  $\{a_1, \dots, a_r\}$  and  $\{b_1, \dots, b_s\}$  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*

$$P(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) = 0 \quad (9)$$

$$Q(t, e^{a_1 t}, \dots, e^{a_r t}, e^{ib_1 t}, \dots, e^{ib_s t}) = 0 \quad (10)$$

have no common solution  $t \in \mathbb{R} \setminus \{0\}$ .

PROOF. Consider a solution  $t \neq 0$  of Equations (9) and (10). 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,

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

Thus, dividing  $P$  and  $Q$  by  $R$ , we may assume that  $P$  and  $Q$  are coprime in  $\mathcal{A}$  and that Equations (9) and (10) still hold.

Since coprime univariate polynomials cannot have a common root, we may assume without loss of generality that  $r + s \geq 1$ . By Schanuel's Conjecture, the field

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

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

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

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

Equations (9) and (10) say that  $S$  is 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 entry of  $S$  corresponding to  $\sigma$  (where  $t$  corresponds to  $x$ ,  $e^{a_j t}$  to  $y_j$ , and  $e^{b_j t}$  to  $z_j$ ) is algebraic over the remaining entries of  $S$ . We claim that these remaining entries 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  $\sigma$  does not appear in  $Q$  (for then  $Q$  gives the desired algebraic relation). On the other hand, if  $\sigma$  has positive degree in  $Q$  then, since  $P$  and  $Q$  are coprime in  $\mathcal{A}$ , the multivariate resultant  $\text{Res}_\sigma(P, Q)$  is a non-zero polynomial in which the variable  $\sigma$  does not appear and which vanishes at  $S$  (see, e.g., [9, Page 163]). Thus the claim also holds in this case. We thus obtain a contradiction and conclude that Equations (9) and (10) have no non-zero solution  $t \in \mathbb{R}$ .  $\square$

THEOREM 3.5. *The Bounded Zero Problem is decidable assuming Schanuel's conjecture.*

PROOF. Consider an exponential polynomial

$$f(z) = P(z, e^{a_1 z}, \dots, e^{a_r z}, e^{ib_1 z}, \dots, e^{ib_s z}), \quad (11)$$

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 determine whether  $f$  has a zero in a bounded interval  $I \subseteq \mathbb{R}_{\geq 0}$  with rational endpoints.

If  $r = s = 0$  then  $f(z)$  is a polynomial with algebraic coefficients and deciding the existence root in  $I$  is straightforward.

If  $r$  and  $s$  are not both zero then any root of  $f(z)$  must be transcendental by Theorem 2.2 (see [2, Theorem 8] for details). Thus we may assume without loss of generality that  $I$  is an open interval. We continue by considering separately the cases of Type-1 and Type-2 exponential polynomials.

*Case (i):  $f$  is a Type-1 exponential polynomial.* By assumption  $P$  and  $P^*$  are irreducible and are not associates in  $\mathcal{R}$ . Thus they are coprime in  $\mathcal{R}$ . We claim that the equation  $f(z) = 0$  has no solution  $z \in \mathbb{R}$ . Indeed if  $z \in \mathbb{R}$  is a zero of  $f$  then

$$f^*(z) = \overline{f(\bar{z})} = \overline{f(z)} = 0,$$

that is,  $z$  is a common zero of  $f$  and  $f^*$ . It follows that

$$(z, e^{a_1 z}, \dots, e^{a_r z}, e^{ib_1 z}, \dots, e^{ib_s z})$$

is a common zero of  $P$  and  $P^*$ , contradicting Proposition 3.4.

*Case(ii):  $f$  is a Type-2 exponential polynomial.* We wish to use the zero-finding procedure of Section 3.1 to determine whether  $f$  has a zero in the open interval  $I$ . To this end we must show that the complex zeros of  $f$  come in conjugate pairs and all its real zeros are simple.

Considering complex zeros first, note that by the assumption on  $f$  we have  $P^* = UP$  for some unit  $U \in \mathcal{R}$ . It follows that:

$$\begin{aligned} f(z) = 0 &\Leftrightarrow f^*(z) = 0 && (\text{since } P^* = UP) \\ &\Leftrightarrow \overline{f(\bar{z})} = 0 \\ &\Leftrightarrow f(\bar{z}) = 0. \end{aligned}$$

Thus  $z$  is zero of  $f$  iff  $\bar{z}$  is a zero of  $f$ .

We next show, assuming Schanuel's Conjecture, that the zeros of  $f$  are all simple. We have

$$f'(z) = Q(z, e^{a_1 z}, \dots, e^{a_r z}, e^{ib_1 z}, \dots, e^{ib_s z}),$$

for some polynomial  $Q \in \mathcal{R}$ . We claim that  $P$  and  $Q$  are coprime in  $\mathcal{R}$ . Since  $P$  is irreducible,  $P$  and  $Q$  can only fail to be coprime if  $P$  divides  $Q$ .

If  $P$  has degree  $k > 0$  in  $X$  then  $Q$  has degree  $k - 1$  in  $X$  and thus  $P$  cannot divide  $Q$ . (Recall that all polynomials in  $\mathcal{R}$  have non-negative degree in the variable  $X$ .) On the other hand, if  $X$  does not appear in  $P$  then we can write  $P = \sum_{u,v} \alpha_{u,v} Y^u Z^v$ , where  $\alpha_{u,v} \in \mathbb{C}$  for all  $u \in \mathbb{Z}^r$  and  $v \in \mathbb{Z}^s$ . We then have  $Q = \sum_{u,v} \alpha_{u,v} \beta_{u,v} Y^u Z^v$ , where

$$\beta_{u,v} := \sum_{j=1}^r a_j u_j + i \sum_{j=1}^s b_j v_j.$$

By the rational linear independence of  $\{a_1, \dots, a_r\}$  and  $\{b_1, \dots, b_s\}$ , the numbers  $\beta_{u,v}$  are pairwise distinct and non-zero. Since  $P$  is not a unit, it has at least two monomials. We conclude that  $P$  does not divide  $Q$  and hence  $P$  and  $Q$  are coprime. From Proposition 3.4 we conclude that the equations  $f'(z) = f(z) = 0$  have no solution  $z \in \mathbb{C}$ .  $\square$

#### 4 DECIDABILITY FOR ONE AND TWO INDEPENDENT FREQUENCIES

Define a *frequency* of an exponential polynomial to be the imaginary part of one of its exponents. In the following subsections we consider exponential polynomials with, respectively, one and two rationally linearly independent frequencies. In each case our goal is to determine whether a given exponential polynomial  $f$  has infinitely many real zeros and, if  $f$  has only finitely many zeros, to obtain an effective constant  $T$  such that all positive real zeros of  $f$  lie in the interval  $[0, T]$ .

#### 4.1 One independent frequency

**THEOREM 4.1.** *Let  $f(t) = \sum_{j=1}^k P_j(t)e^{\lambda_j t}$  be an exponential polynomial whose set of frequencies spans a  $\mathbb{Q}$ -vector space of dimension at most one. Then we can determine whether  $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\}$  is bounded and, if so, we can compute an integer  $T$  such that  $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\} \subseteq [0, T]$ .*

**PROOF.** Write  $\lambda_j = a_j + ib_j$ , where  $a_j, b_j$  are real algebraic numbers for  $j = 1, \dots, k$ . By assumption there is a single real algebraic number  $b$  such that each  $b_j$  is an integer multiple of  $b$ . 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

$$f(t) = Q(t, e^{a_1 t}, \dots, e^{a_k t}, \cos(bt), \sin(bt)),$$

for some polynomial  $Q$  with algebraic coefficients.

Write  $R := \{t \geq 0 : \sin(bt) \geq 0\}$  and  $R' := \{t \geq 0 : \sin(bt) \leq 0\}$ . We show how to determine boundedness of  $\{t \in R : f(t) = 0\}$ . The procedure to decide boundedness of  $\{t \in R' : f(t) = 0\}$  can be obtained with minor modifications.

Consider the semi-algebraic set

$$E := \left\{ (u, x) \in \mathbb{R}^{k+1} \times [-1, 1] : Q(u, x, \sqrt{1-x^2}) = 0 \right\}$$

and note that for  $t \in R$  we have  $f(t) = 0$  if and only if  $(t, e^{at}, \cos(bt)) \in E$ , where  $e^{at}$  denotes  $(e^{a_1 t}, \dots, e^{a_k t})$ . Let  $E = C_1 \cup \dots \cup C_m$  be a cell decomposition of  $E$ , and define

$$Z_j = \{t \in R : (t, e^{at}, \cos(bt)) \in C_j\}, \quad j = 1, \dots, m.$$

Then  $\{t \in R : f(t) = 0\} = Z_1 \cup \dots \cup Z_m$ .

Fix  $j \in \{1, \dots, m\}$ . We show how to decide whether  $Z_j$  is bounded and, in case  $Z_j$  is bounded, we show how to compute an upper bound on  $Z_j$ . This suffices to prove the theorem. To this end, write  $D_j \subseteq \mathbb{R}^{k+1}$  for the projection of  $C_j \subseteq \mathbb{R}^{k+2}$  on the first  $k+1$  coordinates. We consider two cases.

The first case is that  $\{t : (t, e^{at}) \in D_j\}$  is bounded. By Proposition 2.9 we can compute an upper bound  $T$  of this set. But then  $T$  is an effective upper bound on the set  $Z_j$ .

The second case is that  $\{t : (t, e^{at}) \in D_j\}$  is unbounded. We claim that  $Z_j$  is also unbounded. Indeed, observe that by Proposition 2.9 the set  $\{t : (t, e^{at}) \in D_j\}$  contains an unbounded interval  $(T, \infty)$ . Note also that, by definition of a cell, there exists a continuous semi-algebraic function  $\xi$  with domain  $D_j$  such that  $(u, \xi(u)) \in C_j$  for all  $u \in D_j$ . Then for all  $t \in R$ ,

$$\begin{aligned} f(t) = 0 &\iff (t, e^{at}, \cos(bt)) \in C_j \\ &\iff (t, e^{at}) \in D_j \wedge \xi(t, e^{at}) = \cos(bt) \\ &\iff t \in (T, \infty) \wedge \xi(t, e^{at}) = \cos(bt). \end{aligned}$$

Now  $\xi(t, e^{at})$  is a continuous function with domain  $(T, \infty)$  that takes values in  $[-1, 1]$ . Furthermore  $R \cap (T, \infty)$  contains infinitely many intervals over which  $\cos(bt)$  runs from  $+1$  to  $-1$ . Thus there are infinitely many  $t \in R$  such that  $\xi(t, e^{at}) = \cos(bt)$  and hence  $f$  has infinitely many zeros in  $Z_j$ .  $\square$

#### 4.2 Two independent frequencies

In this section we consider exponential polynomials whose frequencies span a two-dimensional vector space over  $\mathbb{Q}$ . We show that the Infinite Zeros Problem is decidable under the additional assumption that the coefficient polynomials are all constants. (The results in Section 6 show that dropping this additional assumption would entail significant new results about Diophantine approximation of algebraic numbers.) Our strategy is to reduce the Infinite Zero Problem to the question of whether a linear flow on a two-dimensional torus hits infinitely often a certain shrinking target set.

**THEOREM 4.2.** *Let  $f(t) = \sum_{j=1}^k P_j e^{\lambda_j t}$  be an exponential polynomial whose coefficient polynomials  $P_1, \dots, P_k$  are constant and whose frequencies span a two-dimensional vector space over  $\mathbb{Q}$ . Then we can decide whether  $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\}$  is bounded and, if so, we can compute an integer  $T$  such that  $\{t \in \mathbb{R}_{\geq 0} : f(t) = 0\} \subseteq [0, T]$ .*

**PROOF.** Write  $a_j = \operatorname{Re}(\lambda_j)$  for  $j = 1, \dots, k$ . Let  $b_1, b_2$  be real algebraic numbers, linearly independent over  $\mathbb{Q}$ , such that  $\operatorname{Im}(\lambda_j)$  is an integer linear combination of  $b_1$  and  $b_2$  for  $j = 1, \dots, k$ . For each  $n \in \mathbb{Z}$ ,  $\sin(nb_1 t)$  and  $\cos(nb_1 t)$  can be written as polynomials in  $\sin(b_1 t)$  and  $\cos(b_1 t)$  with integer coefficients, and similarly for  $b_2$ . It follows that we can write  $f$  in the form

$$f(t) = Q(e^{a_1 t}, \dots, e^{a_k t}, \cos(b_1 t), \cos(b_2 t), \sin(b_1 t), \sin(b_2 t))$$

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

Write  $R := \{t \geq 0 : \sin(b_1 t) \geq 0 \wedge \sin(b_2 t) \geq 0\}$ . We show how to decide boundedness of  $\{t \in R : f(t) = 0\}$ . The cases for the other three sign conditions on  $\sin(b_1 t)$  and  $\sin(b_2 t)$  follow *mutatis mutandis*.

Define a semi-algebraic set

$$E := \left\{ (u, x, y) \in \mathbb{R}^k \times [-1, 1]^2 : Q(u, x, y, \sqrt{1-x^2}, \sqrt{1-y^2}) = 0 \right\}.$$

Then for  $t \in R$  we have  $f(t) = 0$  if and only if  $(e^{at}, \cos(b_1 t), \cos(b_2 t)) \in E$ , where  $a = (a_1, \dots, a_k)$ . Now consider a cell decomposition  $E = C_1 \cup \dots \cup C_m$ , and define

$$Z_j := \{t \in R : (e^{at}, \cos(b_1 t), \cos(b_2 t)) \in C_j\}, \quad j = 1, \dots, m, \quad (12)$$

Then  $\{t \in R : f(t) = 0\} = Z_1 \cup \dots \cup Z_m$ . We now analyse the boundedness of each component  $Z_j$ .

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

First suppose that  $\{t \in \mathbb{R} : e^{at} \in D_j\}$  is bounded. Then by Proposition 2.9 we can compute an upper bound  $T$  of this set, entailing that  $Z_j \subseteq [0, T]$ . On the other hand, suppose that  $\{t \in \mathbb{R} : e^{at} \in D_j\}$  is unbounded. Then, by Proposition 2.9, this set contains an unbounded interval  $(T, \infty)$  for some  $T \in \mathbb{N}$ . Write  $I = [-1, 1]$  and define functions  $g_1, g_2, h_1, h_2 : D_j \rightarrow I$  by

$$g_1(u) = \inf\{x \in I : \exists y(u, x, y) \in C_j\} \quad g_2(u) = \inf\{y \in I : \exists x(u, x, y) \in C_j\} \quad (13)$$

$$h_1(u) = \sup\{x \in I : \exists y(u, x, y) \in C_j\} \quad h_2(u) = \sup\{y \in I : \exists x(u, x, y) \in C_j\} \quad (14)$$

These functions are all semi-algebraic, hence by Proposition 2.10 the limits  $g_i^* := \lim_{t \rightarrow \infty} g_i(e^{at})$  and  $h_i^* := \lim_{t \rightarrow \infty} h_i(e^{at})$  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.

*Case I:* Suppose that  $g_1^* = h_1^*$  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 Proposition 2.10 there exist  $T_1, \varepsilon > 0$  such that for all  $t > T_1$  and  $i = 1, 2$ ,

$$|g_i(e^{at}) - g_i^*| < e^{-\varepsilon t} \text{ and } |h_i(e^{at}) - h_i^*| < e^{-\varepsilon t}. \quad (15)$$

Then for  $t \in R$  such that  $t > T_1$  we have

$$\begin{aligned} t \in Z_j &\iff (e^{at}, \cos(b_1 t), \cos(b_2 t)) \in C_j \quad (\text{by (12)}) \\ &\implies g_1(e^{at}) \leq \cos(b_1 t) \leq h_1(e^{at}) \text{ and } g_2(e^{at}) \leq \cos(b_2 t) \leq h_2(e^{at}) \quad (\text{by (13)(14)}) \\ &\implies |\cos(b_1 t) - g_1^*| < e^{-\varepsilon t} \text{ and } |\cos(b_2 t) - g_2^*| < e^{-\varepsilon t} \quad (\text{by (15)}) \end{aligned} \quad (16)$$

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 (16) implies that for some  $k_1, k_2 \in \mathbb{Z}$ ,

$$|b_1 t - \varphi_1 - 2k_1 \pi| < 3e^{-\varepsilon t/3} \text{ and } |b_2 t - \varphi_2 - 2k_2 \pi| < 3e^{-\varepsilon t/3}. \quad (17)$$

Combining the upper bounds in (17) with the polynomial lower bounds from Lemma 2.3 (i.e., that either for some  $N$  and all  $t$  sufficiently large, either  $|b_1 t - \varphi_1 - 2k_1 \pi| > 1/t^N$  or  $|b_2 t - \varphi_2 - 2k_2 \pi| > 1/t^N$ ) we obtain an effective bound  $T_2$  for which  $t \in Z_j$  implies  $t < T_2$ .

*Case II:* Next, suppose that  $g_1^* < h_1^*$ . In this case we show that  $Z_j$  is unbounded. The geometric intuition is as follows: 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  $\Gamma_t := \{(x, y) : (e^{at}, x, y) \in C_j\}$ . Intuitively such a particle must reach  $\Gamma_t$  for arbitrarily large values of  $t$  since its orbit is dense in  $[-1, 1]^2$  and  $\Gamma_t$  “converges” to a subset of  $[-1, 1]^2$  that has positive dimension.

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

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 Proposition 2.10 the limits  $\lim_{t \rightarrow \infty} \xi(e^{at}, c)$  and  $\lim_{t \rightarrow \infty} \xi(e^{at}, d)$  exist and are algebraic numbers in the interval  $[-1, 1]$ . Let  $\theta, \theta' \in [0, \pi]$  be such that  $\cos(\theta) = \lim_{t \rightarrow \infty} \xi(e^{at}, d)$  and  $\cos(\theta') = \lim_{t \rightarrow \infty} \xi(e^{at}, c)$ .

Since  $\cos(\theta), \cos(\theta'), \cos(\psi)$  and  $\cos(\psi')$  are algebraic,  $e^{i(\theta' - \theta)}$  and  $e^{i(\psi' - \psi)}$  are also algebraic, and hence by the Gelfond-Schneider theorem (Theorem 2.1), the quotient  $\frac{\theta' - \theta}{\psi' - \psi}$  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  $\theta''$  with  $\theta < \theta'' < \theta'$ , such that

$$\theta < \theta'' + \frac{b_2}{b_1}(\psi' - \psi) < \theta'. \quad (18)$$

Since  $2\pi, b_1, b_2$  are linearly independent over  $\mathbb{Q}$  it follows from Proposition 2.6 that  $\{(b_1 t, b_2 t) \bmod 2\pi : t \in \mathbb{R}_{\geq 0}\}$  is dense in  $[0, 2\pi)^2$ . Thus there is an increasing sequence  $t_1 < t_2 < \dots$ , with  $b_1 t_n \equiv \psi \bmod 2\pi$  for all  $n$ , such that  $b_2 t_n \bmod 2\pi$  converges to  $\theta''$ . Then, defining  $s_1 < s_2 < \dots$  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 (18),

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

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

$$\begin{aligned} \eta(t) = 0 &\implies \cos(b_2 t) = \xi(e^{at}, \cos(b_1 t)) \\ &\implies (e^{at}, \cos(b_1 t), \cos(b_2 t)) \in C_j \\ &\implies t \in Z_j \text{ (by (12))}. \end{aligned}$$

Now  $\lim_{n \rightarrow \infty} \eta(t_n) = \cos(\theta) - \cos(\theta'') > 0$  and  $\lim_{n \rightarrow \infty} \eta(s_n) < \cos(\theta') - \cos(\theta'') = 0$ . 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.

*Case III:* Finally, the case  $g_2^* < h_2^*$  is symmetric to Case II.  $\square$

## 5 DECIDABILITY UP TO ORDER EIGHT

We now shift our attention to the low-order case. The main results of this section establish decidability of the Infinite Zeros Problem and conditional decidability of the Zero Problem for exponential polynomials of order at most 8.

### 5.1 Known decidable cases

First we recall some simple criteria on the dominant terms of an exponential polynomial that make it easy to decide whether it has infinitely many zeros.

LEMMA 5.1. *Let  $f$  be an exponential polynomial that has a single dominant term that is moreover associated to a real exponent. Then  $f$  has finitely many nonnegative real zeros, all lying in an interval  $[0, T]$  for some effectively computable constant  $T$ .*

PROOF. Suppose that  $f$  has dominant term  $At^d e^{rt}$  for real algebraic numbers  $A \neq 0$  and  $r$  and a nonnegative integer  $d$ . Then we can write  $\frac{f(t)}{e^{rt} t^d} = A + g(t)$ , where  $|g(t)| = O(1/t)$ . Moreover the constants in the asymptotic notation are effective and hence we can compute the desired threshold  $T$ .  $\square$

LEMMA 5.2. [2, Theorem 11] *An exponential polynomial that has no dominant term associated to a real exponent has infinitely many zeros.*

THEOREM 5.3. [2, Theorem 15] *Consider an exponential polynomial whose dominant exponents all have constant coefficients, are at least four in number, and have imaginary parts linearly independent over  $\mathbb{Q}$ . Then the existence of infinitely many zeros is decidable. Moreover, if there are finitely many zeros then there is an effective threshold  $T$  such that all zeros are in  $[0, T]$ .*

### 5.2 Two and three rationally linearly independent frequencies

In this section we consider certain sub-cases of the Infinite Zeros Problem for exponential polynomials of order at most 8 that are not covered by the results of Section 4. Namely, we consider exponential polynomials with two rationally linearly independent frequencies and non-constant coefficients, and exponential polynomials with three rationally linearly independent frequencies.

Lemmas 5.4 and 5.5, below, concern exponential polynomials in which the dominant terms involve linear coefficient polynomials.

LEMMA 5.4. *Let  $A, B, C, D, E, a, b, r_1$  be real algebraic numbers such that  $a, b > 0 > r_1$  and  $A, B \neq 0$ . Let also  $\varphi_1, \varphi_2, \varphi_3 \in \mathbb{R}$  be such that  $e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3}$  are algebraic. Define the exponential polynomial  $f$  by*

$$f(t) = t(A \cos(at + \varphi_1) + B) + (C \cos(at + \varphi_2) + D) + Ee^{r_1 t} \cos(bt + \varphi_3).$$

*Then it is decidable whether  $f$  has infinitely many zeros. Moreover if  $f$  has only finitely many zeros, then there exists an effective constant  $T$  such that all zeros lie in  $[0, T]$ .*

PROOF. We can assume without loss of generality that  $a/b \notin \mathbb{Q}$ , since otherwise  $f$  would have at most one rationally linearly independent frequency and the lemma would follow from Theorem 4.1.

Considering the dominant term  $t(A \cos(at + \varphi_1) + B)$ , it is clear that if  $|A| > |B|$  then  $f$  changes change sign infinitely often, whereas if  $|B| > |A|$ , then for  $t$  large enough,  $f(t)$  has the same sign as  $B$ . Thus, we can assume  $|A| = |B|$ . Dividing  $f$  by  $B$ , and replacing  $\varphi_1$  by  $\varphi_1 + \pi$  if necessary, we can moreover assume that  $f$  has the form:

$$f(t) = \underbrace{t(1 - \cos(at + \varphi_1))}_{\alpha(t)} + \underbrace{(C \cos(at + \varphi_2) + D)}_{\beta(t)} + \underbrace{e^{r_1 t} E \cos(bt + \varphi_3)}_{\gamma(t)}. \quad (19)$$

We now focus on the *critical times*  $t_j \stackrel{\text{def}}{=} \frac{2j\pi - \varphi_1}{a}$ ,  $j \in \mathbb{N}$ , at which the dominant term  $\alpha(t)$  vanishes. Define  $F \stackrel{\text{def}}{=} C \cos(\varphi_2 - \varphi_1) + D$  and notice that  $\beta(t_j) = F$  for all  $j \in \mathbb{N}$ .

Case (i). Suppose that  $F \leq 0$ . By the linear independence of  $a, b$  and Proposition 2.6, we have  $\gamma(t_j) < 0$  for infinitely many  $j$ . Thus  $f(t_j) = F + \gamma(t_j)$  is negative for infinitely many  $j$ . But, considering the dominant term  $\alpha(t)$ , it is also clear that  $\limsup_{t \rightarrow \infty} f(t) > 0$ . We conclude that  $f$  has infinitely many zeros.

*Case (ii).* Suppose that  $F > 0$ . We claim that  $f$  is ultimately positive. Since  $\limsup_{t \rightarrow \infty} f(t) > 0$ , it suffices to show that for  $t$  sufficiently large, if  $f'(t) = 0$  then  $f(t) > 0$ .

Since  $\beta$  is uniformly continuous, there exists  $\delta > 0$  such that for all  $t \in \mathbb{R}_{\geq 0}$  and  $j \in \mathbb{N}$  such that  $|t - t_j| < \delta$  we have  $\beta(t) > F/2$ . Furthermore, since  $f(t) \geq \beta(t) - e^{r_1 t} |E|$ , we have that  $f(t) > 0$  for all sufficiently large  $t \in \mathbb{R}_{\geq 0}$  and  $j \in \mathbb{N}$  such that  $|t - t_j| < \delta$ .

Let  $t$  be such that  $f'(t) = 0$  and choose  $j \in \mathbb{N}$  such that  $|at + \varphi_1 - j\pi| \leq \frac{\pi}{2}$ . If  $j$  is odd then  $\cos(at + \varphi_1) \leq 0$  and hence  $f(t) \geq t + \beta(t) + \gamma(t)$  is positive for  $t$  sufficiently large. Now suppose that  $j$  is even—say  $j = 2k$  for some  $k$ . From the equation  $f'(t) = 0$  we have

$$|at \sin(at + \varphi_1)| = |\cos(at + \varphi_1) - 1 + \beta'(t) + \gamma'(t)| \leq G \quad (20)$$

for some positive constant  $G$ . It follows that

$$\begin{aligned} |t - t_j| &= \frac{1}{a} |at + \varphi_1 - 2k\pi| && \{ \text{defn. of } t_k, j = 2k \} \\ &\leq \frac{2}{a} |\sin(at + \varphi_1 - 2k\pi)| && \{ \text{since } |x| \leq 2|\sin(x)| \text{ for all } x \in [-\frac{\pi}{2}, \frac{\pi}{2}] \} \\ &\leq \frac{2G}{a^2 t} && \{ \text{By (20)} \}. \end{aligned}$$

We conclude that for  $t$  sufficiently large,  $|t - t_j| < \delta$  and hence, as observed above,  $f(t) > 0$ .  $\square$

LEMMA 5.5. *Let*

$$f(t) = t(A_1 + A_2 \cos(at + \varphi)) + A \cos(at + \varphi_1) + B \cos(bt + \varphi_2) + C,$$

where  $a, b, A, B, C, A_1, A_2 \neq 0$  are real algebraic and  $\varphi, \varphi_1, \varphi_2$  are real with  $a, b$  positive and  $e^{i\varphi}, e^{i\varphi_1}, e^{i\varphi_2}$  algebraic. It is decidable whether  $f$  has infinitely many zeros in  $[0, \infty)$ , and if not, then a threshold  $T$  can be computed such that all zeros of  $f$  lie in  $[0, T]$ .

PROOF. We can assume without loss of generality that  $a/b \notin \mathbb{Q}$ , since otherwise the claim follows from Theorem 4.1. If  $|A_1| < |A_2|$ , then  $f$  has infinitely many zeros (consider large  $t$  such that  $\cos(at + \varphi) = \pm 1$ ), whereas if  $|A_1| > |A_2|$ , then the sign of  $f$  will eventually match that of  $A_1$ , so  $f$  has only finitely many zeros. We are left with the case that  $|A_1| = |A_2|$ . Dividing  $f$  through by  $A_1$  and replacing  $\varphi$  by  $\varphi + \pi$  if necessary, we can write the exponential polynomial as:

$$f(t) = \underbrace{t(1 - \cos(at + \varphi))}_{\alpha(t)} + \underbrace{A \cos(at + \varphi_1) + B \cos(bt + \varphi_2) + C}_{\beta(t)}.$$

The analysis centres around the behaviour of  $f$  around the sequence of *critical points*  $t_j \stackrel{\text{def}}{=} \frac{2j\pi - \varphi}{a}$ ,  $j \in \mathbb{N}$ , at which the dominant term  $\alpha(t)$  is zero. We distinguish three cases, based on comparing  $A \cos(\varphi_1 - \varphi) + C$  with  $|B|$ .

*Case (i).* Suppose first that  $A \cos(\varphi_1 - \varphi) + C < |B|$ . We claim that  $f$  has infinitely many zeros. Writing  $\varepsilon = |B| - A \cos(\varphi_1 - \varphi) - C > 0$ , we have

$$\begin{aligned} f(t_j) &= A \cos(\varphi_1 - \varphi) + C + B \cos(bt_j + \varphi_2) \\ &= |B| - \varepsilon + B \cos(bt_j + \varphi_2). \end{aligned}$$

By the linear independence of  $a, b$  and Proposition 2.6, we have that for infinitely many  $j$ ,  $|B| + B \cos(bt_j + \varphi_2) \in [0, \varepsilon/2]$ , say, and hence  $f(t_j) < -\varepsilon/2 < 0$ . Since also  $\limsup_{t \rightarrow \infty} f(t) > 0$ , we conclude that  $f$  has infinitely many zeros, as claimed.

*Case (ii).* Second, suppose that  $A \cos(\varphi_1 - \varphi) + C > |B|$ . We argue that  $f$  has finitely many zeros. To start, we note that for all  $j \in \mathbb{N}$ ,

$$\begin{aligned} \beta(t_j) &= A(\cos(\varphi_1 - \varphi) + C + B \cos(bt + \varphi_2)) \\ &\geq A(\cos(\varphi_1 - \varphi) + C - |B|) \\ &> 0. \end{aligned}$$

Since moreover  $\beta$  is uniformly continuous, there exists  $\delta > 0$  such that  $\beta(t) > 0$  for all  $t \in \mathbb{R}_{\geq 0}$  and  $j \in \mathbb{N}$  such that  $|t - t_j| < \delta$ . In particular, since  $f(t) \geq \beta(t)$  for all  $t$ , we have  $f(t) > 0$  for all  $t$  and  $j$  such that  $|t - t_j| < \delta$ .

Clearly  $\liminf_{t \rightarrow \infty} f(t) > 0$ . Hence to show that  $f$  is ultimately positive, it suffices to show that  $f(t) > 0$  for all sufficiently large  $t$  such that  $f'(t) = 0$ . To this end, let  $t$  be such that  $f'(t) = 0$  and choose  $j \in \mathbb{N}$  such that  $|at + \varphi - j\pi| \leq \frac{\pi}{2}$ . If  $j$  is odd then  $\cos(at + \varphi) \leq 0$  and hence  $f(t) \geq t + \beta(t)$  is positive for  $t$  sufficiently large. Now suppose that  $j$  is even—say  $j = 2k$  for some  $k$ . From the equation  $f'(t) = 0$  we get that

$$|at \sin(at + \varphi)| = |\cos(at + \varphi) - 1 + \beta'(t)| \leq D \quad (21)$$

for some positive constant  $D$ . It follows that

$$\begin{aligned} |t - t_j| &= \frac{1}{a} |at + \varphi - 2k\pi| && \{ \text{defn. of } t_j, j = 2k \} \\ &\leq \frac{2}{a} |\sin(at + \varphi - 2k\pi)| && \{ \text{since } |x| \leq 2|\sin(x)| \text{ for all } x \in [-\frac{\pi}{2}, \frac{\pi}{2}] \} \\ &\leq \frac{2D}{a^2 t}. && \{ \text{By (21)} \}. \end{aligned}$$

Thus for  $t$  sufficiently large,  $|t - t_j| < \delta$  and hence, as observed above,  $f(t) > 0$ .

*Case (iii).* Finally, suppose  $A \cos(\varphi_1 - \varphi) + C = |B|$ . We claim that  $f$  has finitely many zeros if and only if  $\varphi_1 - \varphi = k\pi$  for some  $k \in \mathbb{Z}$ .

Suppose first  $\varphi_1 - \varphi = k\pi$  for some  $k \in \mathbb{Z}$ . Then  $|B| = A \cos(\varphi_1 - \varphi) + C = A(-1)^k + C$ , so

$$\begin{aligned} f(t) &= t(1 - \cos(at + \varphi)) + A \cos(at + \varphi + k\pi) + B \cos(bt + \varphi_2) + C \\ &= (t - A(-1)^k)(1 - \cos(at + \varphi)) + (|B| + B \cos(bt + \varphi_2)). \end{aligned}$$

For  $t \geq |A|$ ,  $f(t) = 0$  is equivalent to

$$\cos(at + \varphi) = 1 \text{ and } \cos(bt + \varphi_2) = -\text{sign}(B),$$

which entails that  $e^{iat}$ ,  $e^{ibt}$  are both algebraic. Then by the Gelfond-Schneider theorem (Theorem 2.1), either  $t = 0$  or  $a/b \in \mathbb{Q}$ , which is a contradiction. Therefore,  $f(t)$  has no zeros  $t \geq |A|$ .

Finally, suppose that  $\varphi_1 - \varphi \neq k\pi$  for all  $k \in \mathbb{Z}$  and  $A \cos(\varphi_1 - \varphi) + C = |B|$ . We claim that  $f$  has infinitely many zeros on  $[0, \infty)$ . Without loss of generality, by replacing  $\varphi_2$  with  $\varphi_2 + \pi$  if necessary, assume that  $B < 0$ . Note also that  $\sin(\varphi_1 - \varphi) \neq 0$ .

By Theorem 2.7, there exist infinitely many  $k \in \mathbb{N}$  such that there exists a corresponding  $l \in \mathbb{N}$  satisfying

$$\left| \frac{b}{a}k - l + \frac{\varphi_2 - \varphi \frac{b}{a}}{2\pi} \right| < \frac{2}{k}. \quad (22)$$

For each such  $k$ , we consider

$$s_k \stackrel{\text{def}}{=} \frac{1}{a} \left( 2k\pi - \varphi + \frac{\delta}{k} \right),$$

where  $\delta$  is a real constant chosen such that  $\text{sign}(\delta A \sin(\varphi_1 - \varphi)) = 1$  and  $|\delta|$  is sufficiently small (to be specified later). We will show that  $f(s_k) \leq 0$  for all sufficiently large  $k$ . Since also  $\limsup_{t \rightarrow \infty} f(t) > 0$ , this suffices to



show that  $f$  has infinitely many zeros. To this end, we will separately bound the terms  $s_k(1 - \cos(as_k + \varphi))$ ,  $A \cos(as_k + \varphi_1)$  and  $B \cos(bs_k + \varphi_2)$  for all  $k$  large enough, and hence bound  $f(s_k)$  from above by zero.

Firstly, we consider the dominant term of  $f(s_k)$ :

$$\begin{aligned}
 s_k(1 - \cos(as_k + \varphi)) &= \frac{2k\pi - \varphi + \frac{\delta}{k}}{a} \left(1 - \cos\left(\frac{\delta}{k}\right)\right) && \{ \text{definition of } s_k \} \\
 &\leq \frac{2k\pi - \varphi + \frac{\delta}{k}}{a} \frac{\delta^2}{2k^2} && \{ s_k > 0 \text{ and } 1 - \cos(x) \leq x^2/2 \} \\
 &\leq \frac{\pi\delta^2}{a} \frac{1}{k} - \frac{\varphi\delta^2}{2a} \frac{1}{k^2} + \frac{\delta^3}{2a} \frac{1}{k^3} && \{ \text{rearranging} \} \\
 &\leq \frac{2\pi\delta^2}{a} \frac{1}{k}. && \{ \text{for large enough } k \}
 \end{aligned} \tag{23}$$

Next we bound the term  $A \cos(as_k + \varphi_1)$ . Here note that for a differentiable function  $f: \mathbb{R} \rightarrow \mathbb{R}$  and  $x_0 \in \mathbb{R}$  such that  $f'(x_0) \neq 0$ , we have  $f(x_0 + \varepsilon) \leq f(x_0) + \varepsilon \frac{f'(x_0)}{2}$  for all  $\varepsilon$  with  $\text{sign}(\varepsilon f'(x_0)) = -1$  and  $|\varepsilon|$  sufficiently small. Applying this observation to  $f(x) = A \cos x$ , for  $|\delta|$  sufficiently small we have

$$\begin{aligned}
 A \cos(as_k + \varphi_1) &= A \cos\left(\varphi_1 - \varphi + \frac{\delta}{k}\right) && \{ \text{definition of } s_k \} \\
 &\leq A \cos(\varphi_1 - \varphi) - \frac{\delta}{k} \frac{A \sin(\varphi_1 - \varphi)}{2}. && \{ \text{sign}(\delta A \sin(\varphi_1 - \varphi)) = 1 \}
 \end{aligned} \tag{24}$$

Finally, we use (22) to bound  $B \cos(bs_k + \varphi_2)$ :

$$\begin{aligned}
 &\cos(bs_k + \varphi_2) && \{ \text{definition of } s_k \} \\
 &= \cos\left(\frac{b}{a} \left(2k\pi - \varphi + \frac{\delta}{k}\right) + \varphi_2\right) && \{ \text{rearranging} \} \\
 &= \cos\left(2\pi \left(\frac{b}{a}k + \frac{\varphi_2 - \frac{b}{a}\varphi}{2\pi}\right) + \frac{b\delta}{ak}\right) && \{ \text{by (22) for some } l \in \mathbb{N} \text{ and } \varepsilon \in \mathbb{R} \text{ with } |\varepsilon| < 2/k \} \\
 &= \cos\left(2\pi(l + \varepsilon) + \frac{b\delta}{ak}\right) && \{ \text{by the inequality } 1 - \cos(x) \leq x^2/2 \text{ for all } x \in \mathbb{R} \} \\
 &\geq 1 - \frac{1}{2} \left|2\pi\varepsilon + \frac{b\delta}{ak}\right|^2 && \{ \text{by the triangle inequality and } |\varepsilon| < 2/k \} \\
 &\geq 1 - \frac{1}{2k^2} \left(4\pi + \frac{b|\delta|}{a}\right)^2.
 \end{aligned}$$

Hence, noting that  $B < 0$ , we have

$$B \cos(bs_k + \varphi_2) \leq B \left(1 - \frac{1}{2k^2} \left(4\pi + \frac{b|\delta|}{a}\right)^2\right). \tag{25}$$

Combining the above three bounds, we have

$$\begin{aligned}
f(s_k) &= s_k(1 - \cos(as_k + \varphi)) + A \cos(as_k + \varphi_1) + B \cos(bs_k + \varphi_2) + C \\
&\quad \{ \text{by (23)(24)(25)} \} \\
&\leq \frac{2\pi\delta^2}{ak} + A \cos(\varphi_1 - \varphi) - \frac{\delta}{2k} A \sin(\varphi_1 - \varphi) + B \left( 1 - \frac{1}{2k^2} \left( 4\pi + \frac{b|\delta|}{a} \right)^2 \right) + C \\
&\quad \{ \text{by } A \cos(\varphi_1 - \varphi) + C = |B| \text{ and } B < 0 \} \\
&= \frac{1}{k} \left( \frac{2\pi\delta^2}{a} - \frac{\delta A \sin(\varphi_1 - \varphi)}{2} \right) - \frac{1}{k^2} \frac{B}{2} \left( 4\pi + \frac{b|\delta|}{a} \right)^2.
\end{aligned}$$

Since  $\text{sign}(\delta A \sin(\varphi_1 - \varphi)) = 1$ , for  $|\delta|$  small enough we have  $\frac{2\pi\delta^2}{a} - \frac{\delta A \sin(\varphi_1 - \varphi)}{2} < 0$ . Then for all large enough  $k$ , since  $1/k^2$  shrinks faster than  $1/k$ , we will have

$$\text{sign}(f(s_k)) = \text{sign} \left( \frac{2\pi\delta^2}{a} - \delta c \right) = -1.$$

Therefore,  $f$  is negative infinitely often and hence has infinitely many zeros, as claimed.  $\square$

LEMMA 5.6. *Let*

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C \cos(ct + \varphi_3) + D) + e^{r_2 t} E,$$

where  $a, b, c, B, C, D, E, r_1, r_2$  are real algebraic,  $e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3}$  are algebraic, at least one of  $D, E$  is equal to zero,  $a, b, c > 0$ ,  $B, C \neq 0$  and  $r_2 < r_1 < 0$ . It is decidable whether  $f$  has infinitely many zeros on  $[0, \infty)$ , and if not, then a threshold  $T$  can be computed such that if  $f(t) = 0$ , then  $t \leq T$ .

PROOF. Since all the coefficient polynomials occurring in  $f$  are constant, if  $\{a, b, c\}$  is not a linearly independent set over  $\mathbb{Q}$  then the claim follows from Theorem 4.2. Thus, we may assume that  $a, b, c$  are linearly independent over the rationals.

Next, we argue that if  $D < |C| + |B|$ , then  $f$  has infinitely many zeros. Indeed, by Proposition 2.6, the linear independence of  $a, b, c$  entails that the trajectory  $(at + \varphi_1, bt + \varphi_2, ct + \varphi_3) \bmod 2\pi$  is dense in  $[0, 2\pi)^3$ , and moreover the restriction of this trajectory to  $at + \varphi_1 \bmod 2\pi = 0$  is dense in  $\{0\} \times [0, 2\pi)^2$ . Thus,  $\{B \cos(bt + \varphi_2) + C \cos(ct + \varphi_3) + D : t \geq 0 \text{ and } at + \varphi_1 \bmod 2\pi = 0\}$  is dense in  $[D - |C| - |B|, D + |C| + |B|]$ . If  $D < |C| + |B|$ , then because  $r_2 < r_1 < 0$ , it will happen infinitely often that

$$\begin{aligned}
1 - \cos(at + \varphi_1) &= 0, \\
e^{r_1 t} (B \cos(bt + \varphi_2) + C \cos(ct + \varphi_3) + D) &< e^{r_1 t} \frac{D - |C| - |B|}{2} < -|E| e^{r_2 t},
\end{aligned}$$

and hence  $f(t) < 0$ . On the other hand,  $f$  is also positive infinitely often, so  $f$  must have infinitely many zeros.

Suppose now that  $D \geq |B| + |C| > 0$ . By the premise of the Lemma,  $E = 0$ , so  $f$  has the form

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C \cos(ct + \varphi_3) + D).$$

We argue that  $f$  has no zeros, except possibly at  $t = 0$ . Indeed, we have  $B \cos(bt + \varphi_2) + |B| \geq 0$  and  $C \cos(ct + \varphi_3) + |C| \geq 0$  for all  $t$ , so  $f(t) \geq 0$  for all  $t$ . Then  $f(t) = 0$  if and only if  $D = |B| + |C|$  and simultaneously

$$\begin{aligned}\cos(at + \varphi_1) &= 1, \\ \cos(bt + \varphi_2) &= -\text{sign}(B), \\ \cos(ct + \varphi_3) &= -\text{sign}(C),\end{aligned}$$

which entails that  $e^{iat}$ ,  $e^{ibt}$ ,  $e^{ict}$  are all algebraic. Therefore, by the Gelfond-Schneider theorem (Theorem 2.1), either  $t = 0$  or  $a, b, c$  are rational multiples of one another. The latter possibility contradicts the linear independence of  $a, b, c$ , so we conclude that  $f$  has at most one zero.  $\square$

LEMMA 5.7. *Let*

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C \cos(bt + \varphi_3) + D) + e^{r_2 t} E,$$

where  $a, b, B, C, D, E, r_1, r_2$  are real algebraic,  $e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3}$  are algebraic, at least one of  $D, E$  is equal to zero,  $a, b > 0$ ,  $B \neq 0$  and  $r_2 < r_1 < 0$ . It is decidable whether  $f$  has infinitely many zeros on  $[0, \infty)$ , and if not, then a threshold  $T$  can be computed such that if  $f(t) = 0$ , then  $t \leq T$ .

PROOF. If  $a/b \in \mathbb{Q}$ , then the claim follows from Theorem 4.1, so assume that  $a, b$  are linearly independent over the rationals. Then by Proposition 2.6, it happens infinitely often that  $1 - \cos(at + \varphi_1) = 0$  and  $Bt \cos(bt + \varphi_2) < -|B|t/2$ , say. For large enough such  $t$ , we will have

$$e^{r_1 t} (Bt \cos(bt + \varphi_2) + C \cos(bt + \varphi_3) + D) + e^{r_2 t} E < 0,$$

hence  $f(t) < 0$ , so  $f$  has infinitely many zeros.  $\square$

LEMMA 5.8. *Let*

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C) + e^{r_2 t} f_2(t),$$

where  $a, b, B, C, r_1, r_2$  are real algebraic,  $e^{i\varphi_1}, e^{i\varphi_2}$  are algebraic,  $a, b > 0$  positive,  $B \neq 0$ ,  $r_2 < r_1 < 0$  and  $f_2$  is an exponential polynomial whose dominant exponents are purely imaginary. Suppose also the order of  $f$  is at most 8. It is decidable whether  $f$  has infinitely many zeros on  $[0, \infty)$ , and if not, then a threshold  $T$  can be computed such that if  $f(t) = 0$ , then  $t \leq T$ .

PROOF. Suppose first  $a/b \in \mathbb{Q}$ . Because of the bound on the order of  $f$ ,  $f_2$  has order at most 3, so it cannot simultaneously have complex exponents and non-constant coefficients. Thus, either  $f$  has at most one linearly independent frequency, or  $f$  has constant coefficients and at most two linearly independent frequencies. Either way, the result follows from Theorems 4.1 and 4.2.

Therefore, assume now that  $a, b$  are linearly independent over  $\mathbb{Q}$ . By Proposition 2.6, the trajectory  $(at + \varphi_1 \bmod 2\pi, bt + \varphi_2 \bmod 2\pi)$  is dense in  $[0, 2\pi)^2$ , and moreover the restriction of this trajectory to  $at + \varphi_1 \bmod 2\pi = 0$  is dense in  $\{0\} \times [0, 2\pi)$ .

If  $|C| < |B|$ , then we argue that  $f$  is infinitely often negative, and hence has infinitely many zeros. Indeed,  $|C| < |B|$  entails the existence of a non-empty interval  $I \subseteq [0, 2\pi)$  such that

$$bt + \varphi_2 \bmod 2\pi \in I \text{ implies } B \cos(bt + \varphi_2) + C < 0.$$

What is more, we can in fact find  $\varepsilon > 0$  and a subinterval  $I' \subseteq I$  such that

$$bt + \varphi_2 \bmod 2\pi \in I' \text{ implies } B \cos(bt + \varphi_2) + C < -\varepsilon.$$

Thus, by density,  $1 - \cos(at + \varphi_1) = 0$  and  $B \cos(bt + \varphi_2) + C < -\varepsilon$  will infinitely often hold simultaneously. Then just take  $t$  large enough to ensure, say,  $|e^{r_2 t} f_2(t)| < \varepsilon/2$  at these infinitely many points, and the claim follows.

If  $|C| > |B|$ , then clearly for all large enough  $t$ , we have

$$\text{sign}(e^{r_1 t}(B \cos(bt + \varphi_2) + C) + e^{r_2 t} f_2(t)) = \text{sign}(C).$$

If  $C < 0$ , then  $f$  has infinitely many zeros (consider  $t$  such that  $\cos(at + \varphi_1) = 1$ ), whilst if  $C > 0$ , then  $f$  is ultimately positive.

Thus, suppose now  $|B| = |C|$ . Replacing  $\varphi_2$  by  $\varphi_2 + \pi$  if necessary, we can write the function as:

$$f(t) = 1 - \cos(at + \varphi_1) + Ce^{r_1 t}(1 - \cos(bt + \varphi_2)) + e^{r_2 t} f_2(t).$$

As  $a, b$  are linearly independent, for all  $t$  large enough,  $1 - \cos(at + \varphi_1)$  and  $1 - \cos(bt + \varphi_2)$  cannot simultaneously be ‘too small’. More precisely, by Lemma 2.3, there exist effective constants  $E, T, N > 0$  such that for all  $t \geq T$ , we have

$$1 - \cos(at + \varphi_1) > E/t^N \text{ or } 1 - \cos(bt + \varphi_2) > E/t^N.$$

Now, if  $C < 0$ , it is easy to show that  $f$  has infinitely many zeros. Indeed, consider the times  $t$  where the dominant term  $1 - \cos(at + \varphi_1)$  vanishes. For all large enough such  $t$ , since  $|1/t^N|$  shrinks more slowly than  $e^{(r_2 - r_1)t}$  and  $|f_2(t)|$  is bounded above by a constant (because its dominant exponents are purely imaginary), we will have

$$\begin{aligned} f(t) &= e^{r_1 t} \left( C(1 - \cos(bt + \varphi_2)) + e^{(r_2 - r_1)t} f_2(t) \right) \\ &< e^{r_1 t} \left( ECt^{-N} + e^{(r_2 - r_1)t} f_2(t) \right) \\ &\leq e^{r_1 t} \frac{1}{2} ECt^{-N} \\ &< 0, \end{aligned}$$

so  $f$  has infinitely many zeros. Similarly, if  $C > 0$ , we can show that  $f$  is ultimately positive. Indeed, for all  $t$  large enough, we have

$$\begin{aligned} f(t) &\geq e^{r_1 t} \left( C(1 - \cos(bt + \varphi_2)) + e^{(r_2 - r_1)t} f_2(t) \right) \\ &> e^{r_1 t} \left( CEt^{-N} + e^{(r_2 - r_1)t} f_2(t) \right) \\ &> \frac{CE}{2} t^{-N} \\ &> 0 \end{aligned}$$

or

$$\begin{aligned} f(t) &\geq 1 - \cos(at + \varphi_1) + e^{r_2 t} f_2(t) \\ &> Et^{-N} + e^{r_2 t} f_2(t) \\ &> \frac{E}{2} t^{-N} \\ &> 0. \end{aligned}$$

Therefore,  $f$  has only finitely many zeros, all occurring up to an effective bound.  $\square$

### 5.3 Main result

We now draw together the lemmas in the previous two subsections to prove the main result of this section.

**THEOREM 5.9.** *It is decidable whether a given exponential polynomial  $f$  of order at most 8 has infinitely many nonnegative real zeros. Moreover, there exists an effective threshold  $T$  computable from the description of  $f$ , such that if  $f$  has only finitely many zeros, then they are all contained in  $[0, T]$ .*

**PROOF.** Suppose we are given an exponential polynomial  $f$  of order at most 8. By dividing  $f$  through by  $e^{rt}$  if necessary, where  $r$  is the real part of the dominant exponents of  $f$ , we may assume without loss of generality that  $r = 0$  and that all non-dominant exponents have strictly negative real part.

Throughout this proof, we will use the following notational conventions. We denote by  $r_1, r_2, \dots$  the real parts of the non-dominant exponents of  $f$ . These are real algebraic numbers such that  $0 > r_1 > r_2 > \dots$ . The lowercase letters  $a, b, c$  will denote frequencies of  $f$ , always real algebraic and strictly positive. Uppercase letters  $A, B, C, \dots$  will denote real algebraic numbers (of arbitrary sign), whilst  $\varphi, \varphi_1, \varphi_2, \varphi_3$  will denote real numbers such that  $e^{i\varphi}, e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3}$  are algebraic. For an exponential polynomial  $f(t) = \sum_{j=1}^m P_j(t)e^{\lambda_j t}$ , we say that exponent  $\lambda_j$  has *multiplicity*  $\text{mul}(\lambda_j) := \deg(P_j)$ .

We will now perform a case analysis on the number of dominant exponents. Throughout, we rely on the equivalent general forms of real-valued exponential polynomials, outlined in Section 2.1. By Lemma 5.2, it is sufficient to confine our attention to exponential polynomials with an odd number of dominant exponents. By Lemma 5.1 above, the claim is already proven for exponential polynomials with a single dominant term, corresponding to a real exponent.

*Case I.* Suppose first that  $f$  has seven dominant exponents: namely 0 and  $\pm ai, \pm bi, \pm ci$  for non-zero real algebraic numbers  $a, b, c$ . The dominant complex exponents must all have multiplicity one since, otherwise the order of  $f$  would exceed 8. If  $\text{mul}(0) > 1$ , then 0 has strictly greater multiplicity than the other dominant exponents and the claim follows from Lemma 5.1. Thus, we can assume all dominant exponents have multiplicity one.

The sum of the multiplicities of the dominant exponents is 7, so  $f$  can have at most one other, necessarily real, exponent without exceeding order 8, and this exponent must necessarily have multiplicity one.

We now consider the dimension of rational vector space spanned by  $\{a, b, c\}$ . If the dimension is at most 2 then the claim follows from Theorems 4.1 and 4.2, whereas if the dimension is 3 then we are done by Lemma 5.3. This completes Case I.

*Case II.* Next, suppose  $f$  has five dominant exponents: 0 and  $\pm ai, \pm bi$  for non-zero real algebraic numbers  $a, b$ . The bound on the order of  $f$  guarantees that  $(\text{mul}(\pm ai), \text{mul}(\pm bi)) \in \{(1, 2), (2, 1), (1, 1)\}$ .

Assume first that  $(\text{mul}(\pm ai), \text{mul}(\pm bi)) = (2, 1)$ . (The case  $(1, 2)$  is symmetric.) If  $\text{mul}(0) \neq 2$ , then the claim follows from Lemma 5.2, since then  $f$  has a single dominant term which corresponds to a non-real exponent. Thus assume that  $\text{mul}(0) = 2$ , so  $f$  is given by:

$$f(t) = t(A_1 + A_2 \cos(at + \varphi)) + A \cos(at + \varphi_1) + B \cos(bt + \varphi_2) + C.$$

The claim is proven for exponential polynomials of this form in Lemma 5.5.

We can now assume that the complex dominant exponents all have multiplicity one:  $\text{mul}(\pm ai) = \text{mul}(\pm bi) = 1$ . If  $\text{mul}(0) > 1$ , then we are done by Lemma 5.1, so assume  $\text{mul}(0) = 1$ . If  $a/b \notin \mathbb{Q}$ , the claim follows from Lemma 5.3, so assume  $a/b \in \mathbb{Q}$ . If  $f$  has no complex exponents other than  $\pm ai$  and  $\pm bi$ , then the  $\mathbb{Q}$ -span of the frequencies of  $f$  has dimension one and the claim follows by Theorem 4.1. On the other hand, if  $f$  has another conjugate pair of complex exponents, say  $r_1 \pm ci$  with  $r_1 < 0$ , then by the order bound of 8,  $f$  has constant coefficients and the  $\mathbb{Q}$ -span of the frequencies has dimension at most two, so the claim follows by Theorems 4.1 and 4.2.

*Case III.* Finally, we can assume that  $f$  has three dominant exponents: one real 0 and a complex pair  $\pm ai$ . By Lemmas 5.1 and 5.2, the claim is proven when  $\text{mul}(0) \neq \text{mul}(\pm ai)$ . Taking into account the order bound on  $f$ ,

we have  $\text{mult}(0) = \text{mult}(\pm ai) \leq 2$ . If  $\text{mult}(0) = \text{mult}(\pm ai) = 2$ , then  $f$  has the form:

$$f(t) = t(A \cos(at + \varphi_1) + B) + (C \cos(at + \varphi_2) + D) + f_1(t),$$

where  $f_1(t)$  is an exponential polynomial of order at most 2 whose exponents have strictly negative real parts. If the exponents of  $f_1$  are both real then the claim follows by Theorem 4.1; otherwise the claim follows from Lemma 5.4.

Suppose now  $\text{mult}(0) = \text{mult}(\pm ai) = 1$ , so  $f$  has the form

$$f(t) = A_1 + A_2 \cos(at + \varphi_1) + f_1(t),$$

where  $f_1$  is an exponential polynomial of order at most 5 whose exponents all have strictly negative real part, so that  $f_1(t)$  tends to 0 exponentially quickly as  $t$  grows to infinity. Notice that if  $|A_1| > |A_2|$ , then  $f$  cannot have infinitely many zeros. Indeed, for  $t$  sufficiently large we will have  $|f_1(t)| < |A_1| - |A_2|$ , and the sign of  $f$  will match that of  $A_1$ . On the other hand, if  $|A_2| > |A_1|$ , then  $f$  will change sign infinitely often. It remains to consider the case that  $|A_1| = |A_2|$ . Moreover, dividing through by  $A_1$  and, if necessary, replacing  $\varphi_1$  by  $\varphi_1 + \pi$ , we can assume without loss of generality that  $A_1 = 1$  and  $A_2 = -1$ , so that

$$f(t) = 1 - \cos(at + \varphi_1) + f_1(t).$$

Since  $f_1(t)$  converges to zero as  $t$  grows to infinity, it is clear that  $\limsup_{t \rightarrow \infty} f(t) > 0$ . Thus,  $f$  has infinitely many zeros if also  $\liminf_{t \rightarrow \infty} f(t) < 0$ .

From here onwards, we proceed by performing a case split on the dominant exponents of  $f_1$ , that is, the exponents of  $f$  of second-greatest real part. (Note in passing that if  $f_1$  is identically zero, then  $f$  has infinitely many zeros, occurring at  $t$  such that  $\cos(at + \varphi_1) = 1$ .) Let the exponents of  $f_1$  have real part  $r_1 < 0$ .

*Case III.1.* Suppose first that the exponents of  $f$  of second-largest real part are five in number, that is, a real frequency  $r_1$  and two pairs of complex exponents  $r_1 \pm bi$ ,  $r_1 \pm ci$ . By the order bound on  $f$ ,  $\text{mult}(r_1 \pm bi) = \text{mult}(r_1 \pm ci) = \text{mult}(r_1) = 1$ , so that  $f$  has the form

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C \cos(ct + \varphi_3) + D).$$

Then the claim follows from Lemma 5.6.

*Case III.2.* Next, suppose that the exponents of  $f$  of second-largest real part are four in number, that is, two pairs of complex exponents  $r_1 \pm bi$ ,  $r_1 \pm ci$ . Then  $f$  is of the form

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C \cos(ct + \varphi_3)) + e^{r_2 t} D.$$

The claim follows from Lemma 5.6.

*Case III.3.* Next, suppose that the exponents of  $f$  of second-largest real part are three in number, a real  $r_1$  and a complex pair  $r_1 \pm bi$  with  $\text{mult}(r_1 \pm bi) \geq 2$ . By the order bound on  $f$ , we must have  $\text{mult}(r_1 \pm bi) = 2$  and  $\text{mult}(r_1) = 1$ , so that  $f$  has the form

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (Bt \cos(bt + \varphi_2) + C \cos(bt + \varphi_3) + D).$$

In this case, the claim follows from Lemma 5.7.

*Case III.4.* Next, suppose that the exponents of  $f$  of second-largest real part are two in number, a complex pair  $r_1 \pm bi$  with  $\text{mult}(r_1 \pm bi) \geq 2$ . By the order bound on  $f$ ,  $\text{mult}(r_1 \pm bi) = 2$  and  $f$  can have at most one other exponent, so that

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (Bt \cos(bt + \varphi_2) + C \cos(bt + \varphi_3)) + De^{r_2 t}.$$

The claim follows from Lemma 5.7.

*Case III.5.* Next, suppose that the exponents of  $f$  of second-largest real part are three in number, a simple complex pair  $r_1 \pm bi$  and a (possibly repeated) real exponent  $r_1$ .

If  $\text{mult}(r_1) > 1$ , then by Lemma 5.1,  $f_1$  is ultimately positive or ultimately negative, depending on the sign of the leading term of the polynomial associated with  $e^{r_1 t}$ . In the former case  $f$  is also ultimately positive, whilst in the latter case,  $f$  has infinitely many zeros since  $f$  is negative for arbitrarily large values of  $t$  (consider large  $t$  for which  $1 - \cos(at + \varphi_1) = 0$ ).

Therefore, assume  $\text{mult}(r_1) = \text{mult}(r_1 \pm bi) = 1$ , so that

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} (B \cos(bt + \varphi_2) + C) + f_2(t),$$

where  $f_2$  is an exponential polynomial of order at most 2 whose dominant exponents have real part  $r_2$  such that  $r_2 < r_1$ . The claim follows from Lemma 5.8.

*Case III.6.* Next, suppose that the exponents of  $f$  of second-largest real part are a simple complex pair  $r_1 \pm bi$ , so that

$$f(t) = 1 - \cos(at + \varphi_1) + e^{r_1 t} B \cos(bt + \varphi_2) + f_2(t),$$

where  $f_2$  is an exponential polynomial of order at most 3 whose dominant exponents have real part strictly smaller than  $r_1$ . Then the result follows from Lemma 5.8.

*Case III.7.* Finally, if the exponents of  $f$  of second-largest real part comprise a single real exponent  $r_1$ , then by Lemma 5.1,  $f_1$  is ultimately positive or ultimately negative, depending on the sign of the leading coefficient of the polynomial associated with  $e^{r_1 t}$ . In the former case,  $f$  is also ultimately positive, whilst in the latter,  $f$  has infinitely many zeros.

This completes the proof.  $\square$

## 6 DIOPHANTINE HARDNESS AT ORDER NINE

In this section we show that decidability of the Infinite Zeros Problem at order 9 would entail significant new effectiveness results in Diophantine approximation, thereby identifying a formidable mathematical obstacle to extending the positive results in Sections 4 and 5. Analogous “mathematical hardness” results can be proven for the Zero Problem (see [6, Chapter 6.4]).

Given a real number  $\alpha$ , its *Lagrange constant* (sometimes called the *homogeneous Diophantine approximation constant*) is defined by

$$L_\infty(\alpha) := \inf \left\{ c > 0 : \left| \alpha - \frac{n}{m} \right| < \frac{c}{m^2} \text{ for infinitely many } m, n \in \mathbb{Z} \right\}.$$

The Lagrange constant measures how well  $\alpha$  can be approximated by rational numbers and is closely related to the simple continued fraction expansion of  $\alpha$ . Specifically, it is shown in [20, pp. 22-23] that if  $\alpha$  is given as a simple continued fraction by the sequence of partial quotients  $(a_j)_{j=1}^\infty$ , so that

$$\alpha = a_1 + \frac{1}{a_2 + \frac{1}{\ddots}},$$

then  $L_\infty(\alpha) > 0$  if and only if the sequence  $(a_j)_{j=1}^\infty$  is bounded and more generally we have  $K(\alpha) \leq L_\infty(\alpha)^{-1} \leq K(\alpha) + 2$ , where  $K(\alpha) = \limsup_{k \geq 1} a_k$ .

Rational numbers have finite simple continued fraction expansions. It is furthermore well-known that the simple continued fraction expansion of every real algebraic number of degree two is periodic and therefore has bounded partial quotients (and thus also a positive Lagrange constant). However nothing is known for real algebraic numbers of degree three or more. 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?*” Equivalently one can ask whether there exists an algebraic number of degree greater than two that has strictly positive Lagrange constant.

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, Theorem 6.4, shows that the existence of a decision procedure for Infinite Zeros Problem entails the computability of  $L_\infty(\alpha)$  for all real algebraic numbers  $\alpha$ . (In fact we would even obtain a single algorithm that inputs real algebraic number  $\alpha$  and rational  $\varepsilon > 0$  and outputs a rational approximation of  $L_\infty(\alpha)$  to within  $\varepsilon$ .) Now one possibility is that the Lagrange constant  $L_\infty(\alpha)$  of every real algebraic number  $\alpha$  of degree greater than two is zero, and hence trivially computable. However the significance of Theorem 6.4 is that in order to prove the decidability of the Infinite Zeros Problem, one would have to establish, *one way or another*, the computability of  $L_\infty(\alpha)$  for every real algebraic number  $\alpha$ .

Let  $\alpha$  be a positive real algebraic number and  $c$  a positive rational number. Consider the following functions:

$$f_1(t) := e^t(1 - \cos t) + \underbrace{t(1 - \cos(\alpha t)) - c \sin(\alpha t)}_{=:g_1(t)} \quad (26)$$

$$f_2(t) := e^t(1 - \cos t) + \underbrace{t(1 - \cos(\alpha t)) + c \sin(\alpha t)}_{=:g_2(t)} \quad (27)$$

$$f(t) := \min(f_1(t), f_2(t)). \quad (28)$$

In this section we prove the following result.

LEMMA 6.1. (1) If  $L_\infty(\alpha) < \frac{c}{2\pi^2}$  then  $f$  has infinitely many zeros.  
 (2) If  $L_\infty(\alpha) > \frac{c}{2\pi^2}$  then  $f(t) = \Omega(\frac{1}{t})$  and so  $f$  has finitely many zeros.

We break down the proof of Lemma 6.1 into several propositions.

PROPOSITION 6.2. Fix  $\varepsilon > 0$  and define  $\kappa_{c,\varepsilon} := \frac{c^2\varepsilon(1+\varepsilon)}{(1-\varepsilon)\pi}$ . Given  $k \in \mathbb{N}$ , let  $2\pi l$  be the closest integer multiple of  $2\pi$  to  $2k\pi\alpha$  and write  $\delta := 2k\pi\alpha - 2\pi l$ . Then the following hold for all  $k$  sufficiently large:

- (1) If  $|\pi k \delta| < c(1 - \varepsilon)$  then  $f(2\pi k) < 0$ .
- (2) If  $|\pi k \delta| > \frac{c(1+\varepsilon)}{(1-\varepsilon)}$  then  $f(2\pi k) > \kappa_{c,\varepsilon} \cdot \frac{1}{k}$ .

PROOF. In general we have

$$\begin{aligned} f(2\pi k) &= 2\pi k(1 - \cos(2\pi k\alpha)) - c|\sin(2\pi k\alpha)| \\ &= 2\pi k(1 - \cos(\delta)) - c|\sin(\delta)|. \end{aligned}$$

We proceed to examine the sign of  $2\pi k(1 - \cos(\delta)) - c|\sin(\delta)|$ .

To show Item 1 we use the following estimates:  $1 - \cos x \leq \frac{1}{2}x^2$  for  $|x| \leq \pi$  and  $(1 - \varepsilon)|x| \leq |\sin x|$  for  $|x| \leq \sqrt{2\varepsilon}$ . For  $k$  sufficiently large, the assumption  $|\pi k \delta| < c(1 - \varepsilon)$  implies that  $|\delta| \leq \sqrt{2\varepsilon}$  and hence

$$\begin{aligned} 2\pi k(1 - \cos(\delta)) - c|\sin(\delta)| &\leq 2\pi k \frac{1}{2}\delta^2 - c(1 - \varepsilon)|\delta| \\ &= |\delta|(\pi k|\delta| - c(1 - \varepsilon)) \\ &< 0. \end{aligned}$$



To show Item 2, suppose that  $|\pi k \delta| > \frac{c(1+\varepsilon)}{(1-\varepsilon)}$ . We will use the estimates  $|\sin x| \leq |x|$  for  $|x| \leq \pi$  and  $(1-\varepsilon)\frac{1}{2}x^2 \leq 1 - \cos x$  for  $|x| \leq \sqrt{2\varepsilon}$ . We consider two cases. If  $|\delta| \leq \sqrt{2\varepsilon}$  then

$$\begin{aligned} 2\pi k(1 - \cos(\delta)) - c|\sin(\delta)| &\geq 2\pi k\frac{1}{2}(1-\varepsilon)|\delta|^2 - c|\delta| \\ &= |\delta|(\pi k(1-\varepsilon)|\delta| - c) \\ &> \frac{c(1+\varepsilon)}{(1-\varepsilon)\pi k}(\pi k(1-\varepsilon)|\delta| - c) \\ &> \frac{c(1+\varepsilon)}{(1-\varepsilon)\pi k}c\varepsilon \\ &= \kappa_{c,\varepsilon} \cdot \frac{1}{k}. \end{aligned}$$

On the other hand, if  $|\delta| > \sqrt{2\varepsilon}$  then  $2\pi k(1 - \cos(\delta)) - c|\sin(\delta)| \geq 2\pi k(1-\varepsilon)\varepsilon - c|\sin(\delta)|$ , which is clearly greater than  $\kappa_{c,\varepsilon} \cdot \frac{1}{k}$  for  $k$  sufficiently large.  $\square$

For all  $k \in \mathbb{N}$  define the interval  $I_{\varepsilon,k} = \{t \in \mathbb{R}_{\geq 0} : |t - 2k\pi| \leq \frac{1}{k^3}\}$ . The following proposition shows that for  $t$  sufficiently large,  $f(t)$  is positive outside  $\bigcup_k I_{\varepsilon,k}$ ; so zeros of  $f$  have to be “sufficiently close” to integer multiples of  $2\pi$ .

**PROPOSITION 6.3.** *For  $t \notin \bigcup_k I_{\varepsilon,k}$  sufficiently large we have  $f(t) > e^{t/2}$ .*

**PROOF.** Given  $t \in \mathbb{R}_{\geq 0}$ , choose  $k \in \mathbb{N}$  so as to minimise  $|t - 2k\pi|$ . Suppose that  $t \notin I_{\varepsilon,k}$ . Then  $\frac{1}{k^3} < |t - 2k\pi| \leq \pi$ . Using the estimate  $1 - \cos x \geq \frac{1}{4}x^2$ , valid for all  $x \in [-\pi, \pi]$ , we have

$$\begin{aligned} f(t) &\geq e^t(1 - \cos t) - c \\ &= e^t(1 - \cos(t - 2k\pi)) - c \\ &\geq e^t\left(1 - \cos\left(\frac{1}{k^3}\right)\right) - c \\ &\geq e^t\frac{1}{4k^6} - c \\ &\geq e^t\frac{1}{4t^6} - c. \end{aligned}$$

But this lower bound is greater than  $e^{t/2}$  for  $t$  sufficiently large.  $\square$

**OF LEMMA 6.1.** We first prove Item 1. Suppose that  $L_\infty(\alpha) < \frac{c}{2\pi^2}$ . Then there exists  $\varepsilon > 0$  such that  $L_\infty(\alpha) < \frac{c(1-\varepsilon)}{2\pi^2}$ . This means that there exist infinitely many positive integers  $k, l$  such that  $|\alpha - \frac{l}{k}| < \frac{c(1-\varepsilon)}{2\pi^2 k^2}$  and hence  $|2\pi k\alpha - 2\pi l| < \frac{c(1-\varepsilon)}{\pi k}$ . Now, applying Item 1 of Proposition 6.2 we deduce that  $f(2\pi k)$  is negative for infinitely many  $k \in \mathbb{N}$ . In view of Proposition 6.3 we conclude that  $f$  has infinitely many zeros.

Towards proving Item 2, suppose that  $L_\infty(\alpha) > \frac{c}{2\pi^2}$ . Then there exists  $\varepsilon > 0$  such that  $L_\infty(\alpha) > \frac{c(1+\varepsilon)}{(1-\varepsilon)2\pi^2}$ . This means that for all  $k$  sufficiently large,  $|\alpha - \frac{l}{k}| > \frac{c(1+\varepsilon)}{(1-\varepsilon)2\pi^2 k^2}$  and hence  $|2\pi k\alpha - 2\pi l| > \frac{c(1+\varepsilon)}{(1-\varepsilon)\pi k}$ . Thus Item 2 of Proposition 6.2 applies.

We want to show that  $f(t) = \Omega(1/t)$ . In view of Proposition 6.3 it will suffice to show that  $f$  is bounded below by a positive-constant multiple of  $\frac{1}{t}$  for all  $t \in I_k$  with  $k$  sufficiently large. To show this we consider the functions  $g_1, g_2$  (see Equations (26) and (27)). Indeed by Item 2 of Proposition 6.2 we have that  $g_1(2k\pi) > \kappa_{c,\varepsilon} \cdot \frac{1}{k}$  for  $k$  sufficiently large. But a direct calculation of the derivative of  $g_1$  shows that for  $k$  sufficiently large we have  $|g'_1(t)| \leq t\alpha + 1 + c \leq 7\alpha k$  for all  $t \in I_k$ . Thus for all  $t \in I_k$  we have

$$g_1(t) \geq \kappa_{c,\varepsilon} \cdot \frac{1}{k} - 7\alpha k \cdot \frac{1}{k^3} = \Omega(1/k) = \Omega(1/t).$$

Exactly the same reasoning applies to  $g_2(t)$  and since  $f \geq \min(g_1, g_2)$  we obtain the desired lower bound for  $f$ .  $\square$

The main result of the section immediately follows from Lemma 6.1.

**THEOREM 6.4.** *Fix a positive real algebraic number  $\alpha$ . If the Infinite Zeros Problem is decidable then  $L_\infty(\alpha)$  can be computed to within arbitrary precision.*

**Remark 6.5.** Let  $g(t) = e^t f(t)$ , where  $f$  is the function defined in Equation (28). Then by Lemma 6.1, if  $L_\infty(\alpha) > \frac{c}{2\pi^2}$  then  $g$  has infinitely many zeros, whereas if  $L_\infty(\alpha) < \frac{c}{2\pi^2}$  then  $g$  diverges to infinity as  $t \rightarrow \infty$ . Thus the ability to decide whether an exponential polynomial of order 9 diverges to infinity in absolute value would also allow to compute the Lagrange constants of real algebraic numbers to arbitrary precision.

## REFERENCES

- [1] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. 2006. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Springer-Verlag.
- [2] Paul C. Bell, Jean-Charles Delvenne, Raphaël M. Jungers, and Vincent D. Blondel. 2010. The continuous Skolem-Pisot problem. *Theoretical Computer Science (TCS)* 411, 40-42 (2010), 3625–3634.
- [3] Jean Berstel and Maurice Mignotte. 1976. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France* 104 (1976), 175–184.
- [4] Edward Bierstone and Pierre D. Milman. 1988. Semianalytic and subanalytic sets. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 67, 1 (1988), 5–42.
- [5] N. Bourbaki. 1966. *Elements of Mathematics: General Topology (Part 2)*. Addison-Wesley.
- [6] V. Chonev. 2015. *Reachability Problems for Linear Dynamical Systems*. Ph. D. Dissertation. University of Oxford.
- [7] Henri Cohen. 1993. *A Course in Computational Algebraic Number Theory*. Springer-Verlag.
- [8] Paul M. Cohn. 2002. *Basic Algebra: Groups, Rings and Fields*. Springer.
- [9] David A. Cox, John Little, and Donal O'Shea. 2007. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer.
- [10] Richard Guy. 2004. *Unsolved Problems in Number Theory* (third ed.). Springer.
- [11] Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhumäki. 2005. Skolem's Problem – On the Border between Decidability and Undecidability. *TUCS Technical Reports* 683 (2005).
- [12] Godfrey H. Hardy and Edward M. Wright. 1999. *An Introduction to the Theory of Numbers*. Vol. 1. Oxford. 979 pages.
- [13] Bettina Just. 1989. Integer Relations Among Algebraic Numbers. In *Mathematical Foundations of Computer Science (MFCS)*, Vol. 379. Springer, 314–320.
- [14] Serge Lang. 1966. *Introduction to Transcendental Numbers*. Reading, Mass (1966).
- [15] D. H. Lehmer. 1961. A Machine Method for Solving Polynomial Equations. *J. ACM* 8, 2 (1961), 151–162.
- [16] Arjen K. Lenstra. 1987. Factoring Multivariate Polynomials over Algebraic Number Fields. *SIAM J. Comput.* 16, 3 (1987), 591–598.
- [17] Angus Macintyre. 2012. Turing meets Schanuel. (2012). Preprint, to appear in the proceedings of Logic Colloquium.
- [18] Angus Macintyre and Alex J Wilkie. 1996. On the Decidability of the Real Exponential Field. (1996).
- [19] David Marker. 2002. *Model Theory: An Introduction*. Springer.
- [20] Wolfgang Schmidt. 1980. Diophantine Approximation. 785 (1980).
- [21] Boris Zilber. 2002. Exponential sums equations and the Schanuel conjecture. *Journal of the London Mathematical Society* 65 (2002), 27–44. Issue 01.
- [22] Boris Zilber. 2005. Pseudo-exponentiation on algebraically closed fields of characteristic zero. *Annals of Pure and Applied Logic* 132, 1 (2005), 67 – 95.