The Orbit Problem for Parametric Linear Dynamical Systems

Christel Baier
Technische Universität Dresden, Germany

Florian Funke
Technische Universität Dresden, Germany

Simon Jantsch
Technische Universität Dresden, Germany

Toghrul Karimov
MPI-SWS, Germany

Engel Lefaucheux
MPI-SWS, Germany

Florian Luca
Wits University, South Africa; King Abdulaziz University, Saudi Arabia; MPI-SWS, Germany

Joël Ouaknine
MPI-SWS, Germany

David Purser
MPI-SWS, Germany

Markus A. Whiteland
MPI-SWS, Germany

James Worrell
Oxford University, UK

Abstract

We study a parametric version of the Kannan-Lipton Orbit Problem for linear dynamical systems. We show decidability in the case of one parameter and Skolem-hardness with two or more parameters.

More precisely, consider a d-dimensional square matrix M whose entries are algebraic functions in one or more real variables. Given initial and target vectors $u, v \in \mathbb{Q}^d$, the parametric point-to-point orbit problem asks whether there exist values of the parameters giving rise to a concrete matrix $N \in \mathbb{R}^{d\times d}$, and a positive integer $n \in \mathbb{N}$, such that $N^n u = v$.

We show decidability for the case in which M depends only upon a single parameter, and we exhibit a reduction from the well-known Skolem Problem for linear recurrence sequences, suggesting intractability in the case of two or more parameters.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Orbit problem, parametric, linear dynamical systems

1 Introduction

The *Orbit Problem* for linear dynamical systems asks to decide, given a square matrix $M \in \mathbb{Q}^{d\times d}$ and two vectors $u, v \in \mathbb{Q}^d$, whether there exists a natural number n such that $M^n u = v$. The problem was shown decidable (in polynomial time) by Kannan and Lipton [**?**] over ten years after Harrison first raised the question of decidability [**?**]. The current paper is concerned with a generalisation of the Orbit Problem to *parametric* linear dynamical systems. In general, parametric models address a major drawback in quantitative verification, namely the unrealistic assumption that quantitative data in models are known *a priori* and can be specified exactly. In applications of linear dynamical systems to automated verification, parameters are used to model partially specified systems (e.g., a faulty component with an unknown failure rate, or when transition probabilities are only known up to some bounded precision) as well as to model the unknown environment of a system. Interval Markov chains can also be considered as a type of parametric linear dynamical system.

▶ **Problem 1** (Parametric Orbit Problem). Given a $(d \times d)$-matrix M, initial and target vectors u, v, whose entries are real algebraic functions in ℓ common real variables $X = (x_1, \ldots, x_\ell)$, does there exist $s \in \mathbb{R}^\ell$, i.e., values of the parameters giving rise to a concrete matrix, initial and target $M(s) \in \mathbb{R}^{d\times d}, u(s), u(s) \in \mathbb{R}^d$, and a positive integer $n \in \mathbb{N}$, such that $M(s)^n u(s) = v(s)$?

We prove two main results in this paper. In the case of a single parameter we show that the Parametric Orbit Problem is decidable. On the other hand, we show that the Parametric Orbit Problem is at least as hard as the Skolem Problem—a well-known decision problem for linear recurrence sequences, whose decidability has remained open for many decades. Our reduction establishes intractability in the case of two or more parameters.

Thus our main decidability result is as follows:

▶ **Theorem 2.** *Problem 1 is decidable when there is a single parameter (i.e., $\ell = 1$).*

Theorem 2 concerns a reachability problem in which the parameters are existentially quantified. It would be straightforward to adapt our methods to allow additional constraints on the parameter, e.g., requiring that s lie in a certain specified interval. In terms of verification, a negative answer to an instance of the above reachability problem could be seen as establishing a form of robust safety, i.e., an 'error state' is not reachable regardless of the value of the unknown parameter.

The proof of Theorem 2 follows a case distinction based on properties of the eigenvectors of the matrix M (whose entries are functions) and the shape of the Jordan normal form J of M. Our theorem assumes the entries of the matrix, initial and target are real algebraic functions—in particular encompassing polynomial and rational functions. Note that even if we were to restrict the entries of M to be polynomials in the parameters, we would still require (complex) algebraic functions in the Jordan normal form. We assume a suitable effective representation of algebraic functions that supports evaluation at algebraic points, computing the range and zeros of the functions, arithmetic operations, and extracting roots of polynomials whose coefficients are algebraic functions.

The most challenging cases arise when J is diagonal. In this situation we can reformulate the problem as follows: given algebraic functions $\lambda_i(x), \gamma_i(x)$ for $1 \leq i \leq t$, does there exist $(n, s) \in \mathbb{N} \times \mathbb{R}$ such that

$$\lambda_i^n(s) = \gamma_i(s) \qquad \text{for all} \qquad i = 1, \ldots, t? \tag{1}$$

A further key distinction in analysing the problem in Equation (1) involves the rank of the multiplicative group generated by the functions $\lambda_1, \ldots, \lambda_t$. To handle the case that the group has rank at least two, a central role is played by the results of Bombieri, Masser, and Zannier (see [**?**, Theorem 2] and [**?**]) concerning the intersection of a curve in $\mathbb{C}^m$, with algebraic subgroups of $(\mathbb{C}^*)^m$ of dimension at most $m - 2$. To apply these results we view the problem in Equation (1) geometrically in terms of whether a curve

$$C = \{(\lambda_1(s), \ldots, \lambda_t(s), \gamma_1(s), \ldots, \gamma_t(s)) : s \in \mathbb{R}\} \subseteq \mathbb{C}^{2t}$$

intersects the multiplicative group

$$G_n = \{(\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t) \in (\mathbb{C}^*)^{2t} \colon \alpha_1^n = \beta_1 \wedge \cdots \wedge \alpha_t^n = \beta_t\}$$

for some $n \in \mathbb{N}$. The above-mentioned results of Bombieri, Masser, and Zannier can be used to derive an upper bound on n such that $C \cap G_n$ is non-empty under certain conditions on the set of multiplicative relations holding among $\lambda_1, \ldots, \lambda_t$ and $\gamma_1, \ldots, \gamma_t$.

We provide specialised arguments for a number of cases for which the results of Bombieri, Masser, and Zannier cannot be applied. In particular, for the case that the multiplicative group generated by the functions $\lambda_1, \ldots, \lambda_t$ has rank one, we provide in Section 6 a direct elementary method to find solutions of Equation (1).

Another main case in the proof is when matrix J has a Jordan block of size at least 2, i.e., it is not diagonal (see Section 4.2). The key instrument here is the notion of the Weil height of an algebraic number together with bounds that relate the height of a number to the height of its image under an algebraic function. Using these bounds we obtain an upper bound on the $n \in \mathbb{N}$ such that the equation $M(s)^n u(s) = v(s)$ admits a solution $s \in \mathbb{R}$.

Related work

Reachability problems in (unparametrized) linear dynamical systems have a rich history. Answering a question by Harrison [?], Kannan and Lipton [?] showed that the point-to-point reachability problem in linear dynamical systems is decidable in PTIME. They also noticed that the problem becomes significantly harder if the target is a linear subspace—a problem that still remains open, but has been solved for low-dimensional instances [?]. This was extended to polytope targets in [?], and later further generalized to polytope initial sets in [?]. Orbit problems have recently been studied in the setting of rounding functions [?]. In our analysis we will make use of a version of the point-to-point reachability problem that allows matrix entries to be algebraic numbers. In this case the eigenvalues are again algebraic, and decidability follows by exactly the same argument as the rational case (although the algorithm is no longer in PTIME), and is also a special case of the main result of [?].

If the parametric matrix M is the transition matrix of a parametric Markov chain (pMC) [?, ?, ?], then our approach combines *parameter synthesis* with the *distribution transformer semantics*. Parameter synthesis on pMCs asks whether some (or every) parameter setting results in a Markov chain satisfying a given specification, expressed, e.g., in PCTL [?]. An important problem in this direction is to find parameter settings with prescribed properties [?, ?, ?], which has also been studied in the context of model repair [?, ?]. While all previous references use the standard path-based semantics of Markov chains, the distribution transformer semantics [?, ?, ?] studies the transition behaviour on probability distributions. It has, to the best of our knowledge, never been considered for parametric Markov chains. Our approach implicitly does this in that it performs parameter synthesis for a reachability property in the distribution transformer semantics.

The Skolem Problem asks whether a linear recurrence sequence $(u_n)_n$ has a zero term (n such that $u_n = 0$). Phrased in terms of linear dynamical systems, the Skolem Problem asks whether a d-dimensional linear dynamical system hits a $(d-1)$-dimensional hyperplane, and decidability in this setting is known for matrices of dimension at most four [?, ?]. A continuous version of the Skolem Problem was examined in [?]. With the longstanding intractability of the Skolem Problem in general, it has recently been used as a reference point for other decision problems [?, ?, ?].

Ostafe and Shparlinski [?] consider the Skolem Problem for parametric families of simple linear recurrences. More precisely, they consider linear recurrences of the form $u_n = a_1(x)\lambda_1(x)^n + \cdots + a_k(x)\lambda_k^n(x)$ for rational functions $a_1, \ldots, a_k, \lambda_1, \ldots, \lambda_k$ with coefficients in a number field. They show that the existence of a zero of the sequence (u_n) can be decided for all values of the parameter outside an exceptional set of numbers of bounded height (note that any value of the parameter such that the sequence u_n has a zero is necessarily algebraic).

2 Preliminaries

We denote by $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \overline{\mathbb{Q}}$ the real, complex, rational, and algebraic numbers respectively. For a field K and a finite set X of variables, $K[X]$ and $K(X)$ respectively denote the ring of polynomials and field of rational functions with coefficients in K. A meromorphic function[1] $f\colon U \to \mathbb{C}$ where U is some open subset $U \subseteq \mathbb{C}^\ell$ is called algebraic, if $P(x_1, \ldots, x_\ell, f(x_1, \ldots, x_\ell)) = 0$ for some $P \in \mathbb{Q}[x_1, \ldots, x_\ell, y]$. We say that f is *real algebraic* if it is real-valued on real inputs.

▶ **Definition 3.** *A* parametric Linear Dynamical System *(pLDS) of* dimension $d \in \mathbb{N}$ *is a tuple* $\mathcal{M} = (X, M, u)$*, where* X *is a finite set of* parameters*,* M *is the* parametrized matrix *whose entries are real algebraic functions in parameters* X *and* u *is the parametric initial distribution whose entries are also real algebraic functions in parameters* X*.*

Given $s \in \mathbb{R}^{|X|}$, we denote by $M(s)$ the matrix $\mathbb{R}^{d\times d}$ obtained from M by evaluating each function in M at s, provided that this value is well-defined. Likewise we obtain $u(s)$. We call $(M(s), u(s))$ the induced linear dynamical system (LDS). The *orbit* of the LDS $(M(s), u(s))$ is the set of vectors obtained by repeatedly applying the matrix $M(s)$ to $u(s)$: $\{u(s), M(s)u(s), M(s)^2u(s), \ldots\}$. The LDS $(M(s), u(s))$ *reaches* a target $v(s)$ if $v(s)$ is in the orbit, *i.e.* there exists $n \in \mathbb{N}$ such that $M(s)^n u(s) = v(s)$.

We remark that $M(s)$ is undefined whenever any of the entries of M is undefined. For any fixed n, the elements of M^n are polynomials in the entries of M, and consequently, M^n is defined on the same domain as M.

Unless we state that M is a constant function, all matrices should be seen as functions, with parameters $x_1, \ldots, x_{|X|}$, or simply x if there is a single parameter. The notation s is used for a specific instantiation of x. We often omit x when referring to a function, either the function is declared constant or when we do not need to make reference to its parameters.

2.1 Computation with algebraic numbers

Throughout this note we employ notions from (computational) algebraic geometry and algebraic number theory. Our approach relies on transforming the matrices we consider in Jordan normal form. Doing so, the coefficients of the computed matrix are not rational anymore but algebraic. Next we recall the necessary basics and refer to [**?**, **?**] for more background on notions utilised throughout the text.

The algebraic numbers $\overline{\mathbb{Q}}$ are the complex numbers which can be defined as some root of a univariate polynomial in $\mathbb{Q}[x]$. In particular, the rational numbers are algebraic numbers. For every $\alpha \in \overline{\mathbb{Q}}$ there exists a unique monic univariate polynomial $P_\alpha \in \mathbb{Q}[x]$ of minimum degree for which $P_\alpha(\alpha) = 0$. We call P_α the *minimal polynomial* of α. An algebraic number α is represented as a tuple $(P_\alpha, \alpha^*, \varepsilon)$, where $\alpha^* = a_1 + a_2 i$, $a_1, a_2 \in \mathbb{Q}$, is an approximation of α, and $\varepsilon \in \mathbb{Q}$ is sufficiently small such that α is the unique root of P_α within distance ε of α^* (such ε can be computed by the root-separation bound, due to Mignotte [**?**]). This is referred to as the *standard* or *canonical representation* of an algebraic number. Given canonical representations of two algebraic numbers α and β, one can compute canonical representations of $\alpha + \beta$, $\alpha\beta$, and α/β, all in polynomial time.

▶ **Definition 4** (Weil's absolute logarithmic height)**.** *Given an algebraic number* α *with minimal polynomial* p_α *of degree* d*, consider the polynomial* $a_d p_\alpha$ *with* $a_d \in \mathbb{N}$ *minimal such that for* $a_d p_\alpha = a_d x^d + \cdots + a_1 x + a_0$ *we have* $a_i \in \mathbb{Z}$ *and* $\gcd(a_1, \ldots, a_d) = 1$*. Write* $a_d p_\alpha = a_d(x - \alpha^{(1)}) \cdots (x - \alpha^{(d)})$*, where* $\alpha^{(1)} = \alpha$*. Define the* (Weil) height $h(\alpha)$ *of* $\alpha \neq 0$ *by* $h(\alpha) = \frac{1}{d}\Big(\log a_d + \sum_{i=1}^{d} \log(\max\{|\alpha^{(i)}|, 1\})\Big)$*. By convention* $h(0) = 0$*.*

[1] A ratio of two holomorphic functions, which are complex-valued functions complex differentiable in some neighbourhood of every point of the domain.

For all $\alpha, \beta \in \overline{\mathbb{Q}}$ and $n \in \mathbb{Z}$ we have from [?, Chapt. 3]:

1. $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2$;
2. $h(\alpha\beta) \leq h(\alpha) + h(\beta)$;
3. $h(\alpha^n) = |n| \cdot h(\alpha)$.

In addition, for $\alpha \neq 0$ we have $h(\alpha) = 0$ if and only if α is a root of unity (α is a root of unity if there exists $k \in \mathbb{N}$, $k \geq 1$, such that $\alpha^k = 1$). Notice that the set of algebraic numbers with both height and degree bounded is always finite.

2.2 Univariate algebraic functions

Let K be an algebraic extension of a field L such that the characteristic polynomial of $M \in L^{d\times d}$ splits into linear factors over K. It is well-known that we can factor M over K as $M = C^{-1}JC$ for some invertible matrix $C \in K^{d\times d}$ and block diagonal Jordan matrix $J = \langle J_1, \dots, J_N\rangle \in K^{d\times d}$. Each block J_i associated with some eigenvalue λ_i, and J_i^n, have the following *Jordan block* form for some $k \geq 1$:

$$J_i = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix} \qquad \text{and} \qquad J_i^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots & \binom{n}{k-1}\lambda^{n-k+1} \\ 0 & \lambda^n & n\lambda^{n-1} & \cdots & \binom{n}{k-2}\lambda^{n-k+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n\lambda^{n-1} \\ 0 & 0 & 0 & \cdots & \lambda^n \end{pmatrix}.$$

Furthermore, each eigenvalue λ of M appears in at least one of the Jordan blocks.

In case $L = \mathbb{Q}$, we may take K to be an algebraic number field. In particular, the eigenvalues of a rational matrix are algebraic. However, in this paper, the entries of our matrix are *algebraic functions*, and so too are the entries in Jordan normal form. We recall some basics of algebraic geometry and univariate algebraic functions required for the analysis in the single-parameter setting, and refer the reader to [?, ?] for further information.

Let $U \subseteq \mathbb{C}$ be a connected open set and $f : U \to \mathbb{C}$ a meromorphic function. We say that f is *algebraic over* $\mathbb{Q}(x)$ if there is a polynomial $P(x, y) \in \mathbb{Q}[x, y]$ such that $P(x, f(x)) = 0$ for all $x \in U$ where f is defined. Notice that a univariate algebraic function has finitely many zeros and poles, and furthermore, these zeros and poles (or zeros at ∞) are algebraic. Indeed, let $P(x, y) = a_d(x)y^d + \dots + a_1(x)y + a_0(x)$, with $a_i \in \mathbb{Q}[x]$, be irreducible. Assuming that f vanishes at s, we have that $a_0(s) = 0$. There are only finitely many s for which this can occur. Furthermore, the function $1/f$ is meromorphic (on a possibly different domain U) and satisfies $y^d P(x, 1/y) = a_d(x) + \ldots + a_1(x)y^{d-1} + a_0(x)y^d$. We conclude that a pole of f (a zero of $1/f$) is a zero of $a_d(x)$.

Let $P(x, y) = \sum_{i=0}^{d} a_i(x)y^i \in \mathbb{Q}(x)[y]$. We say that $c \in \mathbb{C}$ is a *critical point* of P if either $a_d(c) = 0$ or the resultant $\mathrm{Res}_y(P, \frac{\partial P}{\partial y})$ vanishes at c. If P is irreducible, then it has only finitely many critical points since the resultant is a univariate non-zero polynomial.

Let M be a $(d \times d)$-matrix with univariate real algebraic functions as entries. Let its characteristic polynomial be $P(x, y) := \det(Iy - M)$ and write $c_1, \dots, c_m \in \mathbb{C}$ for the critical points of the irreducible factors of P. Then there exist a connected open subset $U \subseteq \mathbb{C}$ such that $\mathbb{R} \setminus \{c_1, \dots, c_m\} \subseteq U$, and d holomorphic functions $\lambda_1, \dots, \lambda_d : U \to \mathbb{C}$ (not necessarily distinct) such that the characteristic polynomial P of M factors as

$$P(x, y) = (y - \lambda_1(x))(y - \lambda_2(x)) \cdots (y - \lambda_d(x))$$

for all points $x \in U$ (see, e.g., [?, Chapt. 1, Thm. 8.9]).

Let us fix a $(d \times d)$-matrix M and vectors u, v with univariate real algebraic entries. We thus have $M \in L^{d\times d}$, $u, v \in L^d$, for some finite field extension L of $\mathbb{Q}(x)$. Let $\mathbb{K}$ be fixed to an algebraic extension of L such that the characteristic polynomial of M splits into linear factors over the field $\mathbb{K}$. Then, over the field $\mathbb{K}$ we have the factorisation $M = C^{-1}JC$ with J in Jordan form. The eigenvalues of M, denoted $\lambda_1, \ldots, \lambda_k$, appear in the diagonal of J. Let the set of exceptional points, denoted $\mathcal{E}$, consist of the finite set $\{c_1, \ldots, c_m\}$, the poles of the entries of M, C, C^{-1}, J, u and v, and points where $\det C(s) = 0$ (i.e., $C(s)$ is singular).

Consider now a non-constant univariate algebraic function λ not necessarily real. In our analysis, we shall need to bound the height $h(\lambda(s))$ in terms of $h(s)$, as long as s is not a zero or a pole of λ. The following lemma shows $h(\lambda(s)) = \Theta(h(s))$ (proof in Appendix A):

▶ **Lemma 5.** *Let λ be a non constant algebraic function in $\mathbb{K}$. Then there exist effective constants $c_1, c_2, c_3, c_4 > 0$ such that for algebraic s not a zero or pole of λ we have* $c_1 h(s) - c_2 \leq h(\lambda(s)) \leq c_3 h(s) + c_4$.

2.2.1 Multiplicative relations

Let $Y = \{\lambda_1, \ldots, \lambda_t\} \subset \mathbb{K}$ be a set of univariate algebraic functions.

▶ **Definition 6.** *A tuple $(a_1, \ldots, a_t) \in \mathbb{Z}^t$ for which $\lambda_1^{a_1} \cdots \lambda_t^{a_t} = 1$ identically, is called a* multiplicative relation*. A set of multiplicative relations is called* independent *if it is $\mathbb{Z}$-linearly independent as a subset of $\mathbb{Z}^t$. The set Y is said to be* multiplicatively dependent *if it satisfies a non-zero multiplicative relation. Otherwise Y is* multiplicatively independent*. The* rank *of Y, denoted* $\operatorname{rank} Y$*, is the size of the largest multiplicatively independent subset of Y.*

A tuple $(a_1, \ldots, a_t) \in \mathbb{Z}^t$, for which there exists $c \in \overline{\mathbb{Q}}$ such that $\lambda_1^{a_1} \cdots \lambda_t^{a_t} = c$ identically, is called a multiplicative relation modulo constants*. We say that Y is* multiplicatively dependent modulo constants *if it satisfies a non-zero multiplicative relation modulo constants. Otherwise Y is* multiplicatively independent modulo constants*.*

In particular, if $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle = 1$, then for each pair λ_i, λ_j, we have $\lambda_i^b = \lambda_j^a$ for some integers a, b not both zero. In the analysis that follows, we only need to distinguish between this case and $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle \geq 2$. We will also need to find multiplicative relations modulo constants between algebraic functions. These can be algorithmically determined and constructed as a consequence of the following proposition. To this end, let L and $L' \subseteq \mathbb{Z}^t$ be the set of multiplicative relations and multiplicative relations modulo constants on Y, respectively. Both L and L' are finitely generated as subgroups of $\mathbb{Z}^t$ under vector addition.

▶ **Proposition 7.** *Given a set $Y = \{\lambda_1, \ldots, \lambda_t\}$ of univariate algebraic functions, one can compute a generating set for both L and L'.*

Proof. This is essentially a special case of a result from [**?**]. Indeed, in Sect. 3.2, they show how to find the generators of the group L in case the λ_i are elements of a finitely generated field over $\mathbb{Q}$. We apply the result to the field $\mathbb{Q}(x, \lambda_1, \ldots, \lambda_t)$ to obtain the claim for the set L. For L', Case 3 of [**?**, Sect. 3.2] computes a generating set as an intermediate step in the computation of a basis of L. Specifically, L and L' are the respective kernels of the maps φ and $\tilde{\varphi}$ in [**?**, Sect. 3.2]. We give an alternative proof sketch specialised to univariate functions in Appendix A. ◀

3 The Multi-Parameter Orbit Problem is Skolem-hard

The *Skolem Problem* asks, given a order-k linear recurrence sequence $(u_n)_n$, uniquely defined by a recurrence relation $u_n = a_1 u_{n-1} + \cdots + a_k u_{n-k}$ for fixed $a_1, \ldots, a_k$ and initial points $u_1, \ldots, u_k$, whether there exists an n such that $u_n = 0$. The problem is famously not known to be decidable for orders at least 5, and problems which the Skolem problem reduce to are said to be *Skolem-hard*. We will now reduce the Skolem at order 5 to the two-parameter parametric orbit problem.

It suffices to only consider the instances of Skolem Problem at order 5 of the form $u_n = a\lambda_1^n + \overline{a\lambda^n} + b\lambda_2^n + \overline{b\lambda_2^n} + c\rho^n = 0$ with $|\lambda_1| = |\lambda_2| \geq |\rho|$ and $a, b, \lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$, $c, \rho \in \overline{\mathbb{Q}} \cap \mathbb{R}$, as the instances of the Skolem Problem at order 5 that are not of this form are known to be decidable [?]. We may assume that $c = \rho = 1$ by considering the sequence $(u_n/c\rho^n)$ if necessary. We can also rewrite $u_n = A\mathrm{Re}\lambda_1^n + B\mathrm{Im}\lambda_1^n + C\mathrm{Re}\lambda_2^n + D\mathrm{Im}\lambda_2^n + 1$ for $A, B, C, D \in \overline{\mathbb{Q}} \cap \mathbb{R}$.

Let $u_n = a\lambda_1^n + \overline{a\lambda_1^n} + b\lambda_2^n + \overline{b\lambda_2^n} + 1 = A\mathrm{Re}\lambda_1^n + B\mathrm{Im}\lambda_1^n + C\mathrm{Re}\lambda_2^n + D\mathrm{Im}\lambda_2^n + 1$ be a hard instance of the Skolem Problem. Let $M = \mathrm{diag}\left(\begin{bmatrix}\mathrm{Re}\lambda_1 & -\mathrm{Im}\lambda_1 \\ \mathrm{Im}\lambda_1 & \mathrm{Re}\lambda_1\end{bmatrix}, \begin{bmatrix}\mathrm{Re}\lambda_2 & -\mathrm{Im}\lambda_2 \\ \mathrm{Im}\lambda_2 & \mathrm{Re}\lambda_2\end{bmatrix}\right)$, that is, the Real Jordan Normal Form of $\mathrm{diag}(\lambda_1, \overline{\lambda_1}, \lambda_2, \overline{\lambda_2})$. We set the starting point to be $u = [1\ 1\ 1\ 1]^\top$ and show how to define parametrized target vectors $v_1(s,t), \ldots, v_k(s,t)$ such that for all n, $u_n = 0$ if and only if there exist $s, t \in \mathbb{R}$ such that $M^n s = v_i(s,t)$ for some i. The Skolem Problem at order 5 then reduces to k two-parameter orbit problems.

The idea of our reduction is to first construct a semiagebraic set $Z \subseteq \mathbb{R}^4$, $Z = \bigcup_{i=1}^k Z_i$ such that $u_n = 0$ if and only if $(\mathrm{Re}\lambda_1^n, \mathrm{Im}\lambda_1^n, \mathrm{Re}\lambda_2^n, \mathrm{Im}\lambda_2^n) \in Z$, and each Z_i is a semialgebraic subset of $\mathbb{R}^4$ that can be described using two parameters and algebraic functions in two variables. Observing that $M^n s = (Re\lambda_1^n - \mathrm{Im}\lambda_1^n, \mathrm{Im}\lambda_1^n + \mathrm{Re}\lambda_1^n, Re\lambda_2^n - \mathrm{Im}\lambda_2^n, \mathrm{Im}\lambda_2^n + \mathrm{Re}\lambda_2^n)$, we then compute $v_i(s,t)$ from Z_i as follows. Suppose $Z_i = \{(x(s,t), y(s,t), z(s,t), u(s,t) : s, t. \in \mathbb{R}\}$. Then $v_i(s,t) = (x(s,t) - y(s,t), y(s,t) + x(s,t), u(s,t) - v(s,t), v(s,t) + u(s,t))$.

To compute Z, first observe that $\mathrm{Im}\lambda_2^n = \pm\sqrt{(\mathrm{Re}\lambda_1^n)^2 + (\mathrm{Im}\lambda_1^n)^2 - (\mathrm{Re}\lambda_2^n)^2}$ for all n as $|\lambda_1| = |\lambda_2|$. Motivated by this observation, let $S_+, S_- \subseteq \mathbb{R}^3$, $S_+ = \{(x,y,z) : Ax + By + Cz + D\sqrt{x^2 + y^2 - z^2} + 1 = 0\}$ and $S_- = \{(x,y,z) : Ax + By + Cz - D\sqrt{x^2 + y^2 - z^2} + 1 = 0\}$. We will choose $Z = \{(x, y, z, \sqrt{x^2 + y^2 - z^2}) : (x,y,z) \in S_+\} \cup \{(x, y, z, -\sqrt{x^2 + y^2 - z^2}) : (x,y,z) \in S_-\}$. It is easy to check that the above definition of Z satisfies the requirement that $u_n = 0$ if and only if $(\mathrm{Re}\lambda_1^n, \mathrm{Im}\lambda_1^n, \mathrm{Re}\lambda_2^n, \mathrm{Im}\lambda_2^n) \in Z$, and it remains to show to that both S_+ and S_- can be parametrized using algebraic functions in two variables and two parameters. To this end, observe that S_+ and S_- are both semialgebraic subsets of $\mathbb{R}^3$, but are also contained in the algebraic set $S = \{(x,y,z) : (Ax + By + Cz + 1)^2 = D^2(x^2 + y^2 - z^2)\} \subseteq \mathbb{R}^3$. Since $S \neq \mathbb{R}^3$ (for example, $(0,0,0) \notin S$), and it is algebraic, S can have *dimension* (see [?] for a definition) at most 2. Hence S_+, S_- also have semialgebraic dimension at most 2. In Appendix B, we show that a semialgebraic subsets of $\mathbb{R}^3$ of dimension at most two can be written as a finite union of sets of the form $\{v(s,t) : s, t \in \mathbb{R}\}$, where v is an algebraic function. This completes the construction of Z and the description of the reduction.

4 Single Parameter Reachability: Overview of proof

In this section we show how to prove Theorem 2, that is, it is decidable, given a $(d \times d)$-matrix M, initial and target vectors u, v, whose entries are real algebraic functions all depending on a single parameter, whether there exist $s \in \mathbb{R}$ giving rise to a concrete matrix, initial and target $M(s) \in \mathbb{R}^{d\times d}, u(s), u(s) \in \mathbb{R}^d$, and a positive integer $n \in \mathbb{N}$, such that $M(s)^n u(s) = v(s)$.

In our case analysis, we often reduce to one of the following two cases, for which decidability is apparent:

▶ **Proposition 8.**

- *Given a finite set $S \subset \mathbb{R}$ it is decidable if there exists $(n, s) \in \mathbb{N} \times S$ s.t. $M(s)^n u(s) = v(s)$.*
- *Given $B \in \mathbb{N}$ it is decidable if there exists $n \leq B$ and $s \in \mathbb{R}$ s.t. $M(s)^n u(s) = v(s)$.*

Proof. The decidability of the first case is a consequence of the fact that a choice of parameter leads to a concrete matrix, thus giving an instance of the non-parametric Orbit Problem.

In the second case, for fixed n, one can observe that the matrix M^n is itself a matrix of real algebraic functions. Hence the equation $M^n u = v$ can be rewritten as equations $P_i(x) = 0$ for real algebraic P_i for $i = 1, \ldots, d$. For each equation the function is either identically zero, or vanishes at only finitely many s which can be determined, and one can check if there is an s in the intersection of the zero sets as i varies. Repeat for each $n \leq B$. ◀

Observe that either there is some n for which $M^n u = v$ holds, or for each n there is a finite number of s such that $M(s)^n u(s) = v(s)$. In the latter case, there are at most countably many s for which there exists n such that $M(s)^n u(s) = v(s)$. Further, all such points are algebraic, as they must be the roots of the algebraic functions P_i.

Our approach will be to place the problem into Jordan normal form (Section 4.1), where we will observe that the problem can be handled immediately if the resulting form is not diagonal (Section 4.2). In the diagonal case the problem can be reformulated for algebraic functions λ_i, γ_i for $i = 1 \ldots, t$, whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda_i^n(s) = \gamma_i(s)$ for all $i = 1, \ldots, t$, where $\mathcal{E}$ is the finite set of exceptional points which can be handled separately (using Proposition 8).

To show decidability we will distinguish between the case where $\mathrm{rank}\langle \lambda_1, \ldots, \lambda_t \rangle$ is 1 and when it is greater than 2 (recall Definition 6). As discussed in the introduction, the most intriguing part of our development will be in the case of $\mathrm{rank}\langle \lambda_1, \ldots, \lambda_t \rangle \geq 2$, captured in the following lemma:

▶ **Lemma 9.** *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$ and $\mathrm{rank}\langle \lambda_1, \ldots, \lambda_t \rangle \geq 2$. Given algebraic functions $\gamma_1, \ldots, \gamma_t$ in $\mathbb{K}$, then it is decidable whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that*

$$\lambda_i(s)^n = \gamma_i(s) \qquad \text{for all} \qquad i = 1, \ldots, t. \tag{2}$$

It will then remain to prove the lemma for the case where the rank is 1. Here we will exploit the initial use of real algebraic functions, to ensure the presence of complex conjugates.

▶ **Lemma 10.** *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$ and $\mathrm{rank}\langle \lambda_1, \ldots, \lambda_t \rangle = 1$. We assume that, if λ_i is complex then $\overline{\lambda_i}$ (the complex conjugate) also appears. Given algebraic functions $\gamma_1, \ldots, \gamma_t$ in $\mathbb{K}$, then it is decidable whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda_i^n(s) = \gamma_i(s)$ for all $i = 1, \ldots, t$.*

In the remainder of this section we will show how to place the problem in the form of these two lemmas: first placing the matrix into Jordan normal form, eliminating the cases where the Jordan form is not diagonal and provide some simplifying assumptions. We then prove Lemmas 9 and 10 in Sections 5 and 6 respectively.

4.1 The parametric Jordan normal form

For every $s \in \mathbb{R} \backslash \mathcal{E}$ we have $M(s) = C^{-1}(s) J(s) C(s)$ and hence, for every $n \in \mathbb{N}$, $M^n(s) u(s) = v(s)$ if and only if $J^n(s) C(s) u(s) = C(s) v(s)$. On the other hand, deciding whether there exists $s \in \mathcal{E}$ with $M^n(s) u(s) = v(s)$ reduces to finitely many instances of the Kannan-Lipton Orbit Problem, which can be decided separately. We have thus reduced the parametric point-to-point reachability problem to the following one in case of a single parameter:

▶ **Problem 11.** Given a matrix $J \in \mathbb{K}^{d \times d}$ in Jordan normal form, and vectors $\tilde{u}$, $\tilde{v} \in \mathbb{K}^d$, decide whether there exists $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $J^n(s) \tilde{u}(s) = \tilde{v}(s)$.

▶ **Example 12.** Define $M = \begin{pmatrix} x+\frac{1}{2} & 0 & 0 \\ \frac{1}{2}-x & 1-x & 0 \\ 0 & x & 1 \end{pmatrix} \in \mathbb{Q}(x)^{3\times 3}$. Then the characteristic polynomial of M is $\det(yI-M) = (y-1/2-x)(y-1)(y+x-1)$. The irreducible factors have no critical points. Now over $\mathbb{K}$ we may write $M = C^{-1}JC$, where $J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-x & 0 \\ 0 & 0 & x+\frac{1}{2} \end{pmatrix}$, $C = \begin{pmatrix} 1 & 1 & 1 \\ \frac{1-2x}{4x-1} & -1 & 0 \\ \frac{2x}{1-4x} & 0 & 0 \end{pmatrix}$, and $C^{-1} = \begin{pmatrix} 0 & 0 & \frac{1}{2x}-2 \\ 0 & -1 & 1-\frac{1}{2x} \\ 1 & 1 & 1 \end{pmatrix}$. Notice that J is defined for all x, while C is not defined at $1/4$, and C^{-1} is not defined at 0 (notice also that $C(0)$ is not invertible). Therefore $\mathcal{E} = \{0, 1/4\}$. For $s \in \mathbb{R}\setminus\mathcal{E}$, all three are defined and we have $M(s) = C^{-1}(s)J(s)C(s)$, with $J(s)$ in Jordan normal form and $C(s)$ invertible.

Notice, for $1/4 \in \mathcal{E}$, we have $M(1/4) = R^{-1}KR$, where $K = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{4} & 1 \\ 0 & 0 & \frac{3}{4} \end{pmatrix}$ and $R = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & 0 \\ -\frac{1}{4} & 0 & 0 \end{pmatrix}$. Notice here that $M(1/4)$ is non-diagonalisable (over $\overline{\mathbb{Q}}$), though M is (over $\mathbb{K}$).

Let $u = (u_1, u_2, u_3) \in \mathbb{Q}(x)^3$ and $v = (v_1, v_2, v_3) \in \mathbb{Q}(x)^3$. The problem of whether there exists $(n, s) \in \mathbb{N} \times \mathbb{R}$ for which $M(s)^n u(s) = v(s)$ is reduced to checking the problem at $s \in \mathcal{E}$, and to the associated problem $J^n(s)\tilde{u}(s) = \tilde{v}(s)$, where $\tilde{u} = \begin{pmatrix} u_1+u_2+u_3 \\ \frac{1-2x}{4x-1}u_1 - u_2 \\ \frac{2x}{1-4x}u_1 \end{pmatrix}$, $\tilde{v} = \begin{pmatrix} v_1+v_2+v_3 \\ \frac{1-2x}{4x-1}v_1 - v_2 \\ \frac{2x}{1-4x}v_1 \end{pmatrix}$, and $J^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (1-x)^n & 0 \\ 0 & 0 & (x+\frac{1}{2})^n \end{pmatrix}$.

Let us establish some notation: assume $J = \langle J_1, \dots, J_N \rangle$, corresponding to eigenvalues $\lambda_1, \dots, \lambda_N$. Assume the dimension of Jordan block J_i is d_i, and let $\tilde{u}_{i,1}, \dots, \tilde{u}_{i,d_i}$ be the coordinates of $\tilde{u}$ associated with the Jordan block J_i, where index 1 corresponds to the bottom of the block. Similarly, let $\tilde{v}_{i,1}, \dots, \tilde{v}_{i,d_i}$ be the corresponding entries of the target.

Let us define the functions $\gamma_1, \dots, \gamma_N$ used in our reduction to Lemma 9 and Lemma 10. We let $\gamma_i(s) = \tilde{v}_{i,1}(s)/\tilde{u}_{i,1}(s)$, for $\tilde{u}_{i,1}(s) \neq 0$. If $\tilde{u}_{i,1}$ is not constant zero, then there are finitely many s where $\tilde{u}_{i,1}(s) = 0$, each of which can be handled explicitly. If some $\tilde{u}_{i,1}$ is the constant zero function, then there are two cases. Firstly, if $\tilde{v}_{i,1}$ is also the constant zero then we are in the degenerate case $\lambda_i^n \cdot 0 = 0$, and the row can be ignored. Secondly if $\tilde{v}_{i,1}$ is not constant zero, then there are only a finite number of s s.t. $0 = \tilde{v}_{i,1}(s)$. Each of these can be checked explicitly.

We say that an eigenvalue $\lambda \in \mathbb{K}$ (possibly constant) is a *generalised root of unity* if there exists an $a \in \mathbb{N}_{\geq 1}$, such that $\lambda^a(x)$ is a real-valued and non-negative function. Let $\mathrm{order}(\lambda)$ of a generalised root of unity λ be the minimal such a. Notice that any real function is a generalised root of unity with order at most 2. When we say an eigenvalue *is* a root of unity, then the eigenvalue is necessarily a constant function.

▶ **Lemma 13.** *To decide Problem 11 it suffices to assume that no λ_i is identically zero and that any λ_i which is a generalised root of unity is real and non-negative (in particular, the only roots of unity are exactly 1).*

Proof. If $\lambda_i = 0$, then $J_i^{d_i+n} = 0$ for all $n \in \mathbb{N}$, hence we only need to check $n \leq d_i$ and the s such that $\tilde{v}_{i,1}(s) = \cdots = \tilde{v}_{i,d_i}(s) = 0$ (unless this holds identically, in which case the constraints from this Jordan block can be removed).

Take $L = \mathrm{lcm}\{\mathrm{order}(\lambda_i) \mid \lambda_i \text{ is generalised root of unity}\}$. Then the reachability problem reduces to L problems: $(J^L)^n(J^k\tilde{u}(x)) = \tilde{v}(x)$ for every $k \in \{0, \dots, L-1\}$. The eigenvalue λ_i^L corresponding to $(J_i)^L$ is now real and non-negative if it is a generalised root of unity. ◀

4.2 Jordan cells of dimension larger than 1

First, we show decidability of the problem when some Jordan block has dimension at least 2:

▶ **Proposition 14.** *If there exists J_i such that $d_i > 1$, then Problem 11 is decidable.*

There are three cases not covered by the previous section: λ_i is not constant, λ_i is constant but not a root of unity, and $\lambda_i = 1$.

Let us start with the case where $\lambda_i \neq 1$, that is λ_i is a constant but not 1, or λ_i is not a constant. Here we can use the bottom two rows from the block to obtain:

$$\lambda_i^n(x)\tilde{u}_{i,1}(x) = \tilde{v}_{i,1}(x) \quad \text{and} \quad \lambda_i^n(x)\tilde{u}_{i,2}(x) + n\lambda_i^{n-1}(x)\tilde{u}_{i,1}(x) = \tilde{v}_{i,2}(x),$$

We reformulate these equations, defining algebraic function θ:

$$\lambda_i^n(x) = \gamma_i(x) = \tilde{v}_{i,1}(x)/\tilde{u}_{i,1}(x) \quad \text{and} \quad n = \theta(x) = \lambda_i(x)(\tilde{v}_{i,2}(x)/\tilde{v}_{i,1}(x) - \tilde{u}_{i,2}(x)/\tilde{u}_{i,1}(x))$$

Any roots or poles of $\tilde{u}_{i,1}, \tilde{u}_{i,2}, \tilde{v}_{i,1}, \tilde{v}_{i,2}, \lambda_i$ can be handled manually (and we already ensured $\tilde{u}_{i,1}$ is not identically zero). We can then apply the following lemma.

▶ **Lemma 15.** *Given algebraic functions λ, γ, θ in parameter x, with λ not a root of unity, then there is a bound on $n \in \mathbb{N}$ such that there exists an $s \in \overline{\mathbb{Q}}$ with $n = \theta(s)$ and $\lambda^n(s) = \gamma(s)$.*

Proof sketch. We sketch the case where λ is not a constant function, a similar (but distinct) approach is used for λ constant. Taking heights on $\lambda^n(s) = \gamma(s)$ we obtain $nh(\lambda(s)) = h(\gamma(s))$, applying Lemma 5 twice (on both λ and γ) we obtain $nh(s) = \Theta(h(s))$. In particular if n is large (say $n > A$) then $h(s)$ is bounded (say $h(s) < B$). Taking heights on $n = \theta(s)$ we obtain $\log(n) = h(\theta(s)) = \Theta(h(s))$. If $n > A$ then $\log(n) \leq BC$. Hence $n \leq \max\{A, exp(BC)\}$. ◀

The remaining case where $\lambda_i = 1$ results only in an equation of the form $n = \theta(s)$, so $\lambda_j^n(s) = \gamma_j(s)$ can be taken from any other Jordan block where $\lambda_j \neq 1$ and again we apply Lemma 15 to place a bound on n.

4.3 Further simplifying assumptions for diagonal matrices

Henceforth, we may assume that J is a diagonal matrix resulting in the formulation of Lemmas 9 and 10: given eigenvalues $\lambda_1, \ldots, \lambda_t$ and so we want to know if there exists $(n, s) \in \mathbb{N} \setminus \mathcal{E}$ such that

$$\lambda_i^n(s) = \gamma_i(s) \qquad \text{for all} \qquad i = 1, \ldots, t \tag{3}$$

Finally we make some simplifications in Lemma 16:

▶ **Lemma 16.** *To decide Problem 11, it suffices to decide the problem with instances where the eigenvalues λ_i are distinct, that none of the λ_i's are identically zero, that none of the constant λ_i's are roots of unity, and every constant λ_i is associated with non-constant γ_i.*

Proof. Consider first the case that $\lambda_1 = \lambda_2$. If also $\gamma_1 = \gamma_2$ then the equations $\lambda_1^n = \gamma_1$ and $\lambda_2^n = \gamma_2$ are equivalent and one of them can be removed. Otherwise, if $\gamma_1 \neq \gamma_2$, the equations $\lambda_1^n = \gamma_1$ and $\lambda_2^n = \gamma_2$ can only have a common solution for $s \in \mathbb{R}$ with $\gamma_1(s) = \gamma_2(s)$, i.e., we can restrict to a finite set of parameters, in which case the problem becomes decidable.

We have already established, in Lemma 13, that none of the λ_i's are identically zero, and that the only constant root of unity is 1. Indeed if $\lambda_j = 1$ then we have $1^n = \gamma_j(s)$, which holds either at finitely many s or γ_j is the constant 1 and the constraint can be dropped.

If there exists i with constant λ_i (not a root of unity) and constant γ_i then there is at most a single n such that $\lambda_i^n = \gamma_i$. This n can be found using the Kannan-Lipton problem on the single constraint. The remaining constraints can be verified for this n using Proposition 8 to determine if they are simultaneously satisfiable. ◀

4.4 Multiplicative dependencies

To handle cases when the eigenvalues λ_i's are multiplicatively dependent, we often argue as in the following manner. Say $\lambda_1^{a_1} = \lambda_2^{a_2} \cdots \lambda_t^{a_t}$ with $a_1 \neq 0$. Consider the system

$$\lambda_i^{a_i}(s)^n = \gamma_i^{a_i}(s) \qquad \text{for all} \qquad i = 1, \dots, t. \tag{4}$$

It is clear that the set E of solutions (n, s) to (3) is a subset of the set E' of solutions to (4). Furthermore, for $(n, s) \in E'$ we have $\gamma_1^{a_1}(s) = \lambda_1^{a_1 n}(s) = (\lambda_2^{a_2} \cdots \lambda_t^{a_t})^n(s) = \gamma_2^{a_2} \cdots \gamma_t^{a_t}(s)$.

We conclude that if $\gamma_1^{a_1} \neq \gamma_2^{a_2} \cdots \gamma_t^{a_t}$, then there can only be finitely many s solving (4), and the problem becomes decidable. In case $\gamma_1^{a_1} = \gamma_2^{a_2} \cdots \gamma_t^{a_t}$, the first equation in (4) is redundant, and we may remove it. By repeating the process we obtain a system of the form (4) where the λ_i are multiplicatively independent, and the solutions to it contain all the solutions to the original system.

Now we face the problem of separating solutions to (3) from the solutions to (4). If either of the sets $\{n \colon (n, s) \in E'\}$ or $\{s \colon (n, s) \in E'\}$ is finite and effectively enumerable, we can clearly decide whether E is empty or not, utilising either Kannan–Lipton or Proposition 8 finitely many times. This happens in the majority of cases. In the case that both the above sets are unbounded, we bound the suitable n in case $\operatorname{rank}\{\lambda_1, \dots, \lambda_t\} \geq 2$ in Section 5. For the case of $\operatorname{rank}\{\lambda_1, \dots, \lambda_t\} \leq 1$ we give a separate argument in Section 6.

5 The case of $\operatorname{rank}\langle\lambda_1, \dots, \lambda_t\rangle \geq 2$

In this section we recall and prove the following Lemma 9:

▶ **Lemma 9.** *Let $\lambda_1, \dots, \lambda_t$ be algebraic functions in $\mathbb{K}$ and $\operatorname{rank}\langle\lambda_1, \dots, \lambda_t\rangle \geq 2$. Given algebraic functions $\gamma_1, \dots, \gamma_t$ in $\mathbb{K}$, then it is decidable whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that*

$$\lambda_i(s)^n = \gamma_i(s) \qquad \text{for all} \qquad i = 1, \dots, t. \tag{2}$$

By Lemma 16 we may assume that none of λ_i's are identically zero or a root of unity.

5.1 All λ_i's constant

In this section we sketch the proof for the case where λ_i's are all constant (the full argument can be found in Appendix D). We reduce to a special case of the Skolem problem, but show that this particular instance is decidable. Since rank ≥ 2, we have at least two constraints and so there are constants λ_1 and λ_2, not roots of unity, and multiplicatively independent, with γ_1, γ_2 not constant.

▶ **Lemma 17.** *Suppose λ_1, λ_2 are constant, not roots of unity, multiplicatively independent, and that γ_1, γ_2 are non-constant functions. Then the system $\lambda_1^n = \gamma_1(s)$, $\lambda_2^n = \gamma_2(s)$ has only finitely many solutions.*

Proof Sketch. Let the minimal polynomials over $\overline{\mathbb{Q}}[x, y]$ of γ_1 and γ_2 be P_1 and P_2 with $P_i \in \overline{\mathbb{Q}}[x, y_i]$. The polynomials P_1 and P_2 have no common factors as elements of $\overline{\mathbb{Q}}[x, y_1, y_2]$. Eliminating x from these polynomials we get a non-zero polynomial $P \in \overline{\mathbb{Q}}[y_1, y_2]$ for which $P(\alpha_1, \alpha_2) = 0$ for all $\alpha_1 = \gamma_1(s)$ and $\alpha_2 = \gamma_2(s)$, $s \in U$. The sequence $(u_n)_{n=0}^{\infty}$, with

$$u_n = P(\lambda_1^n, \lambda_2^n) = \sum_{k,\ell} a_{k,\ell}(\lambda_1^k \lambda_2^\ell)^n,$$

$a_{k,\ell} \in \overline{\mathbb{Q}}$, is a linear recurrence sequence over $\overline{\mathbb{Q}}$, and we wish to characterise those n for which $u_n = 0$. By the famous Skolem–Mahler–Lech theorem (see, e.g., [?]), the set of such n is the union of a finite set and finitely many arithmetic progressions. Furthermore, it is decidable whether such a sequence admits infinitely many elements, and all the arithmetic progressions can be effectively constructed [?]. But, in general, the elements of the finite set are not known to be effectively enumerable—solving the Skolem problem for arbitrary LRS essentially reduces to checking whether this finite set is empty. However, the case at hand can be handled using now standard techniques involving powerful results from transcendental number theory, such as Baker's theorem for linear forms in logarithms, and similar results on linear forms in p-adic logarithms (see, e.g., [?, ?]). We show there exists an effectively computable $n_0 \in \mathbb{N}$ such that $u_n \neq 0$ for all $n \geq n_0$ in Appendix D.1. We give a brief sketch:

Assuming first that $|\lambda_1|$ and $|\lambda_2|$ are multiplicatively independent, it is evident that the modulus of u_n grows as $c\alpha^n + o(\alpha^n)$ for some $c \in \mathbb{R}_+$, where α is the maximal modulus of the terms $\lambda_1^k \lambda_2^\ell$ (there is only one term with this modulus). One can straightforwardly compute an upper bound on any n for which $u_n = 0$.

If the values $|\lambda_1|$ and $|\lambda_2|$ are multiplicatively dependent but neither is of modulus 1, we may again use an asymptotic argument. For this, we need Baker's theorem on linear forms in logarithms to show that a (related) sequence grows in modulus as $c\alpha^n/n^D + o(\beta^n)$, with $\beta < \alpha$ and effectively computable constants c, D. On the other hand, if $|\lambda_i| = 1$ but λ_1 is an algebraic integer (a root of a monic polynomial with coefficients in $\mathbb{Z}$), then it will have a Galois conjugate (roots of the minimal polynomial of λ_1) $\tilde{\lambda_1}$ with $|\tilde{\lambda_1}| > 1$. Hence a suitable Galois conjugate of the sequence (u_n) will be of the form considered in the previous case, and the zeros of (u_n) and $(\tilde{u}_n)$ coincide. The asymptotic argument can be applied to $(\tilde{u}_n)$.

The final case is when λ_1 and λ_2 are not algebraic integers. We turn to the theory of prime ideal decompositions of the numbers λ and argue, employing a version of Baker's theorem for p-adic valuations (see, e.g., [?]) to conclude similarly that the n for which $u_n = 0$ are effectively bounded above. ◀

5.2 At least one non-constant

Henceforth, we can assume that at least one λ_i is non-constant. We may take the λ_i's to be multiplicatively independent with $t \geq 2$, otherwise consider a multiplicatively independent subset of the functions: it always has at least two elements by the assumption on rank, and, furthermore, at least one of them is not constant. The removal of equations will be done as described in Section 4.4; here we show that there are only finitely many n giving solutions (n, s) to the reduced system, so we need not worry about creating too many new solutions.

The following theorems are the main technical results from the literature utilised in the arguments that follow, formulated in a way to suit our needs. Here $\mathcal{C}(\overline{\mathbb{Q}})$ denotes the set of algebraic points in $\overline{\mathbb{Q}}^d$ on an algebraic set $\mathcal{C} \subseteq \mathbb{C}^d$.

▶ **Theorem 18** ([?, Theorem 2]). *Let $\mathcal{C}$ be an* absolutely irreducible *(irreducible in $\overline{\mathbb{Q}}(x)$) curve defined over $\overline{\mathbb{Q}}$ in $\mathbb{C}^d$. Assume that the coordinates of the curve are multiplicatively independent modulo constants (i.e., the points $(x_1, \dots, x_d) \in \mathcal{C}(\overline{\mathbb{Q}})$ do not satisfy $x_1^{a_1} \cdots x_d^{a_d} = c$ identically for any $(a_1, \dots, a_d) \in \mathbb{Z}^d \setminus \vec{0}$, $c \in \overline{\mathbb{Q}}$). Then the points $(x_1, \dots, x_d) \in \mathcal{C}(\overline{\mathbb{Q}})$ for which x_1, …, x_d satisfy at least two independent multiplicative relations form a finite set.*

We note that given the curve $\mathcal{C}$, the finite set of points $(x_1, \dots, x_d)$ on $\mathcal{C}$ for which $x_1, \dots, x_d$, satisfy at least two independent multiplicative relations can be effectively constructed. Indeed, this is explicitly mentioned in the last paragraph of the introduction of [?]: the proof goes by showing an effective bound on the degree and height of such points.

Theorem 18 holds for curves in $\mathbb{C}^d$ for arbitrary d. If one allows the coordinates on the curve to satisfy a non-trivial multiplicative relation, then there can be infinitely many such points [?]. On the other hand, in [?] Bombieri, Masser, and Zannier consider relaxing the assumption of multiplicative independence modulo constants to multiplicative independence and conjecture that the conclusion of the above theorem still holds [?, Conj. A]. Supporting the conjecture, [?] proves a theorem which will suffice for us.

▶ **Theorem 19.** *Let $\mathcal{C}$ be an absolutely irreducible curve in $\mathbb{C}^d$ defined over $\overline{\mathbb{Q}}$. Assume that the the coordinates of the curve are multiplicatively independent, but $\mathcal{C}$ is contained in a set of the form $\vec{b}H$, where H is the set of points in $\overline{\mathbb{Q}}^d$ satisfying at least $d-3$ independent multiplicative relations*[2]*. Then the points $(x_1,\ldots,x_d) \in \mathcal{C}(\overline{\mathbb{Q}})$ for which $x_1, \ldots, x_d$ satisfy at least two independent multiplicative relations form a finite set.*

Again the finite set of points can be effectively computed.[3]

Let us proceed case by case. The proof of the following case is in Appendix D.2.

▶ **Lemma 20.** *Assume that $\{\lambda_1,\ldots,\lambda_t\}$ is multiplicatively dependent modulo constants, but is multiplicatively independent. Then there exists a computable constant n_0 such that system* (2) *admits no solutions for $n > n_0$.*

We may now focus on sets $\{\lambda_1,\ldots,\lambda_t\}$ that are multiplicatively independent modulo constants. We still might have multiplicative dependencies between the λ_i and γ_i. We take care of these cases in the remainder of this section.

▶ **Lemma 21.** *Assume that $\{\lambda_1,\lambda_2,\gamma_1,\gamma_2\}$ is multiplicatively independent. Then system* (2) *admits only finitely many solutions, all of which can be effectively enumerated.*

Proof. We show that the set of s for which the equality can hold is finite and such s can be computed. We employ the powerful Theorems 18 and 19 of Bombieri, Masser, and Zannier, from which the claim is immediate. We first prime the situation as follows.

Let that λ_1, λ_2, γ_1, γ_2 have minimal polynomials $P_1 \in \mathbb{Q}[x,x_1]$, $P_2 \in \mathbb{Q}[x,x_2]$, $P_3 \in \mathbb{Q}[x,x_3]$, $P_4 \in \mathbb{Q}[x,x_4]$, respectively. Eliminating x from P_1 and P_2 (resp., P_3, P_4), we get a polynomial $Q_1 \in \mathbb{Q}[x_1,x_2]$ (resp., $Q_2 \in \mathbb{Q}[x_1,x_3]$, $Q_3 \in \mathbb{Q}[x_1,x_4]$) for which we have $Q_1(\lambda_1(x),\lambda_2(x)) = 0$ (resp., $Q_2(\lambda_1(x),\gamma_1(x)) = 0$, $Q_3(\lambda_1(x),\gamma_2(x)) = 0$) for all x. Let $\mathcal{C}$ be the curve defined by $\mathcal{C} := \{(x_1,x_2,x_3,x_4) \in \mathbb{C}^4 \colon Q_1(x_1,x_2) = Q_2(x_1,x_3) = Q_3(x_1,x_4) = 0\}$ and consider any of its finitely many absolutely irreducible components $\mathcal{C}'$. We are now interested in the pairs of multiplicative relations $(n,0,-1,0)$ and $(0,n,0,-1)$ (corresponding to $x_1^n = x_3$, $x_2^n = x_4$), for $n \geq 1$, along the curve $\mathcal{C}'$. Notice that for any fixed n, these two relations are independent in $\overline{\mathbb{Q}}^4$, i.e., neither is a consequence of the other, as they involve disjoint sets of coordinates.

First assume that $\lambda_1,\lambda_2,\gamma_1,\gamma_2$ are multiplicatively independent modulo constants. Then so is the curve $\mathcal{C}'$, and the result follows from Theorem 18 as the result is constructive.

Otherwise $\lambda_1,\lambda_2,\gamma_1,\gamma_2$ are multiplicatively dependent modulo constants but are multiplicatively independent. Then the points of the curve $\mathcal{C}'$ satsify a multiplicative relation modulo constants $(a_1,\ldots,a_t)$, say $x_1^{a_1}x_2^{a_2}x_3^{a_3}x_4^{a_4} = c$ identically with $c \in \overline{\mathbb{Q}}$ not a root of unity (again, the functions would be multiplicatively dependent were c a root of unity).

[2] With $b = (b_1,\ldots,b_k)$, here $\vec{b}H = \{(b_1x_1,\ldots,b_dx_d) \colon (x_1,\ldots,x_k) \in H\}$ is a coset of a *subgroup of dimension at most* 3 in the terminology of [?].

[3] In [?, ?] the proof is given for $d \geq 4$, and is constructive, while the case of $d = 3$ is attributed to a (non-constructive) result of Liardet [?]. A completely effective proof of the case can be found in [?].

Applying Theorem 19 with $d = 4$, the points on $\mathcal{C}'$ satisfying $x_1^n = x_3$ and $x_2^n = x_4$ for any $n \geq 1$, form an effectively constructable finite set. ◀

To complete the proof of Lemma 9, we need to show the claim holds when $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ are multiplicatively dependent, while λ_1 and λ_2 are multiplicatively independent modulo constants. The proof goes along the same lines as in the above with some extra technicalities. We give the detailed proof in Appendix D.2.

6 The case of $\operatorname{rank}\langle\lambda_1, \ldots, \lambda_t\rangle = 1$

This section recalls and sketches the proof of Lemma 10, with full proofs found in Appendix E.

▶ **Lemma 10.** *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$ and $\operatorname{rank}\langle\lambda_1, \ldots, \lambda_t\rangle = 1$. We assume that, if λ_i is complex then $\overline{\lambda_i}$ (the complex conjugate) also appears. Given algebraic functions $\gamma_1, \ldots, \gamma_t$ in $\mathbb{K}$, then it is decidable whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda_i^n(s) = \gamma_i(s)$ for all $i = 1, \ldots, t$.*

As sketched in Section 4.4, since there is a multiplicative dependence between functions, we first show that, without loss of generality, there is a single equation $\lambda^n(s) = \gamma(s)$.

▶ **Lemma 22.** *Suppose $\operatorname{rank}\langle\lambda_1, \ldots, \lambda_t\rangle = 1$, then whether there is a solution $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ to $\lambda_i^n(s) = \gamma_i(s)$ for all $i = 1, \ldots, t$ reduces to instances with $t = 1$.*

We then separate into the case where λ is real and the case where λ is complex. Let us start by assuming λ is a real function.

▶ **Lemma 23.** *Given real algebraic functions λ and γ, it is decidable whether there exists $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda^n(s) = \gamma(s)$.*

Proof Sketch. The interesting case occurs on an interval $S = (s_0, s_1)$ on which $0 < \lambda(s), \gamma(s) < 1$ for $s \in S$. Other cases either reduce to this case, or occur for finitely many s which can be checked independently. The function $\gamma(s)$ is fixed between s_0, s_1. Each point $\lambda(s)^n$ decreases with every n. One can test for each n whether the lines $\lambda(s)$ and $\gamma(s)$ intersect, or one can find some bound n_0 after which $\lambda(s)^n < \gamma(s)$ for all $s \in S$ and $n > n_0$, so one can be sure there is no solution. ◀

Secondly, we consider the case λ takes on complex values. In this case, since λ_i was a complex eigenvalue of M, then so too is its conjugate $\overline{\lambda_i}$, yet λ_i and $\overline{\lambda_i}$ are multiplicatively dependent, in which case it turns out that $|\lambda| = 1$.

▶ **Lemma 24.** *Let λ and γ be algebraic functions. Assume λ is not real, non-zero, not a root of unity, and of modulus 1. The equation $\lambda(s)^n = \gamma(s)$ admits solutions as follows. If γ is not of modulus* 1 *constantly, then there are finitely many s. If γ is of modulus 1 identically and λ is constant, then there are infinitely many solutions and such a solution can be effectively found. Finally, if λ is not constant, then the equation admits a solution for all $n \geq n_0$, and n_0 is computable.*

Proof Sketch. The interesting case turns outs to be when λ and γ both define arcs on a unit circle. By taking powers of λ the arc grows, and eventually encompasses the arc defined by γ. The intermediate value theorem then implies there is an s satisfying $\lambda^n(s) = \gamma(s)$. ◀

A Additional Material for Section 2

▶ **Proposition 7.** *Given a set $Y = \{\lambda_1, \ldots, \lambda_t\}$ of univariate algebraic functions, one can compute a generating set for both L and L'.*

Proof sketch. An algebraic function λ can be expressed as a converging *Puiseux series* $\lambda(x) = \sum_{n=n_0}^{\infty} c_n(x-\alpha)^{n/\deg_y(P_\lambda)}$ for some $c_n \in \overline{\mathbb{Q}}$, $c_{n_0} \neq 0$, and $n_0 \in \mathbb{Z}$, around a point $\alpha \in \overline{\mathbb{Q}}$ (see [?, Chapt. 1.8.13], [?]). Evidently any $\alpha \in \overline{\mathbb{Q}}$ has *order* $\mathrm{ord}_\lambda(\alpha) = n_0/\deg_y(P_\lambda) \in \mathbb{Q}$, i.e., the exponent of the first term in the Puiseux series. Let $\alpha_1, \ldots, \alpha_k$ be the roots and poles of the λ_i. With each λ_i we associate the vector $g_i = (\mathrm{ord}_{\lambda_i}(\alpha_j))_{j=1}^k$. Now $\sum_{i=1}^k a_i g_i = \vec{0}$ implies that the function $\lambda_1^{a_1} \cdots \lambda_t^{a_t}$ has no roots or poles, hence is constant by Bezout's theorem. Compute a basis for $\ker((g_{i,j})_{i=1,j=1}^{t,k}) \cap \mathbb{Z}^k$ ([?, Cor. 5.3c]) for the claim on L'. As L' is finitely generated, L can be seen as the set of multiplicative relations of a finite set of algebraic numbers. A generating set for L can be found utilising a deep result of Masser [?] ([?, ?]). ◀

▶ **Lemma 5.** *Let λ be a non constant algebraic function in $\mathbb{K}$. Then there exist effective constants $c_1, c_2, c_3, c_4 > 0$ such that for algebraic s not a zero or pole of λ we have*
$c_1 h(s) - c_2 \leq h(\lambda(s)) \leq c_3 h(s) + c_4$.

Proof. To this end, let $P \in \overline{\mathbb{Q}}[x,y]$ be irreducible, with d_x the maximal degree of x, and d_y that of y, and assume $d_x, d_y \geq 1$. Let $P(\alpha, \beta) = 0$ with algebraic α, β. It is known that there exists a constant C_P depending on P such that

$$\left| \frac{h(\alpha)}{d_y} - \frac{h(\beta)}{d_x} \right| \leq C_P \sqrt{\max\left\{\frac{h(\alpha)}{d_y}, \frac{h(\beta)}{d_x}\right\}}.$$

For example, the main result of [?] shows that

$$C_P = 5\left(\log\left(2^{\min\{d_x,d_y\}}(d_x+1)(d_y+1)\right) + h_p(P)\right)^{1/2}$$

suffices[4], and hence an upper bound for C_P is computable, given P.

Now let P be the minimal polynomial of λ. We have for all admissible s: $P(s, \lambda(s)) = 0$. Since λ is not constant, we have that the polynomial contains both x and y, and we may apply the above to get

$$\left| \frac{h(s)}{d_y} - \frac{h(\lambda(s))}{d_x} \right| \leq C_P \sqrt{\max\{h(s)/d_y, h(\lambda(s))/d_x\}}.$$

By taking $c_1 = d_x/(2d_y), c_3 = 2d_x/d_y$ and $c_2 = c_4 = 4C_P^2 \max\{d_x, d_y\}$, we have

$$c_1 h(s) - c_2 \leq h(\lambda(s)) \leq c_3 h(s) + c_4.$$ ◀

B Additional Material for Section 3

In this section we show that each semialgebraic $S \subseteq \mathbb{R}^3$ can be written as a finite union of sets of the form $\{v(s,t) : s, t \in \mathbb{R}\}$.

[4] Here $h_p(P)$ is the *height of the polynomial* P (see [?, Equation (4)]). For us it suffices to know that $h_p(P)$ is at most the sum of the heights of the non-zero coefficients of the polynomial.

One way to define dimension of a semialgebraic set is using *cell decomposition*. We have that a semialgebraic set $S \subseteq \mathbb{R}^3$ of dimension 2 can be written as a finite union of 2-cells and 1-cells in $\mathbb{R}^3$, and that a d-cell is semialgebraically homeomorphic to the open hypercube $(0,1)^d$ [**?**]. Hence to show our main result it suffices to show how to write $C \subseteq \mathbb{R}^3$, $C = f((0,1)^d)$ where f is a semialgebraic function, as a union of sets parametrised using two parameters and algebraic functions in two variables.

First, let us consider parametrisation of very simple sets in $\mathbb{R}$. Observe that a point $p \in \overline{\mathbb{Q}}$ can be characterised using the algebraic function $f(s) = p$, the interval $(0,1]$ as $\{\frac{1}{1+s^2} : s \in \mathbb{R}\}$ and the interval $(0,\infty)$ as $\{\frac{1}{s^2} : s \in \mathbb{R}\}$. We can characterise other intervals using these characterisations. For example, $(a,b] = \{a + \frac{b-a}{1+s^2}\}$, $[b,a) = \{a - \frac{a-b}{1+s^2} : s \in \mathbb{R}\}$ and an open interval (a,b) can be written as $(a,b) = (a, \frac{a+b}{2}] \cup [\frac{a+b}{2}, b)$.

Next, a couple of useful lemmas.

▶ **Lemma 25.** *Let $g \colon \mathbb{R} \mapsto \mathbb{R}$ be a semialgebraic function. The graph $G = \{(x, g(x) \colon x \in \mathbb{R}\}$ can be written as a union of sets of the form $\{v(s) \colon s \in \mathbb{R}\}$.*

Proof. By definition, the function g is semialgebraic if and only if its graph G is a semialgebraic subset of $\mathbb{R}^2$. Let $p_1(x,y) = 0, q_1(x,y) > 0, \ldots, q_m(x,y) > 0$ be the constraints that define G (recall that one can define a semialgebraic set using only one equality constraint). Viewing $p_1, q_1, \ldots, q_m$ as polynomials in y, we can factorise

$$\begin{cases} p_1(x,y) = (y - h_1^0(x)) \cdot \ldots \cdot (y - h_{\kappa(0)}^0(x)) = 0 \\ q_1(x,y) = (y - h_1^1(x)) \cdot \ldots \cdot (y - h_{\kappa(1)}^1(x)) > 0 \\ \cdots \\ q_m(x,y) = (y - h_1^m(x)) \cdot \ldots \cdot (y - h_{\kappa(m)}^m(x)) > 0 \end{cases}$$

where h_r^i is an algebraic function for every $0 \le i \le m$ and $1 \le r \le \kappa(i)$. Next we will show how to compute $\kappa(0)$ subsets $I_1, \ldots, I_{\kappa(0)}$ of $\mathbb{R}$ that have the following properties.

1. $\bigcup_{j=1}^{\kappa(0)} I_j = \mathbb{R}$;
2. Each I_j is a finite union of intervals;
3. For $1 \le j \le \kappa(0)$, the value of y for each $x \in I_j$ is equal to $h_j^0(x)$, the jth root of p_1.

This will allow us to write

$$G = \bigcup_{j=1}^{\kappa(0)} \{(x, h_j^0(x)) : x \in I_j\}.$$

Recall that each I_j is a finite union of intervals, each of which can be parametrised by an algebraic function with domain $\mathbb{R}$. Since composition of two algebraic functions remains algebraic, we can characterise each component of G that comes from a single subinterval of I_j using an algebraic function with domain $\mathbb{R}$. Hence we can write G as a union of sets with the desired parametrization.

To construct I_j, we proceed as follows. From Condition 3 above, $I_j = \{x : (x, h_j^0(x)) \in G\}$ and hence can be defined by the formula

$$\varphi(s) = p_1(x, h_j^0(x)) = 0 \wedge q_1(x, h_j^0(x)) > 0 \wedge \cdots \wedge q_m(x, h_j^0(x)) > 0.$$

Hence I_j is semialgebraic. Since semialgebraic sets have finitely many connected components, I_j must be a finite union of interval subsets of $\mathbb{R}$. ◀

▶ **Lemma 26.** *Let $D \subseteq \mathbb{R}^2$ be semialgebraic. D can be written as*

$$D = \bigcup_{i=1}^{k} D_i = \bigcup_{i=1}^{k} \{v_i(s,t) : s,t \in \mathbb{R}\}$$

where for each i, v_i is algebraic over $\mathbb{Q}(s,t)$.

Proof. By cell decomposition, D must be a union of

1. points,
2. sets of the form $\{(x, g(x)) : x \in (a,b)\}$ where $g : \mathbb{R} \to \mathbb{R}$ is semialgebraic, and
3. sets of the form $\{(x,y) : x \in (a,b), g(x) < y < h(x)\}$ where g, h are semialgebraic.

Sets of the last kind are bands between the graphs of g and h over the open interval (a,b). We need to show that sets of each kind can be parametrized using two parameters and algebraic functions in two variables. The first two cases are handled by the preceding arguments. For the third case, let (a,b), the graph of G and the graph of H be parametrized by the one-variable algebraic functions v_1, v_2 and v_3, respectively. Then the sets of the third type can be written as $\{(v_1(s), v'(s,t)) : s,t \in \mathbb{R}\}$ where $v'(s,t)$ parametrizes the open interval $(g(s), h(s))$ based on the discussion above about parametrizing intervals in $\mathbb{R}$. ◀

Finally, we are ready to prove our main result. Let $C \subseteq \mathbb{R}^3$, $C = f((0,1)^2)$ where f is a semialgebraic function. Let (u,v) denote a point in $(0,1)^2$ and $x(u,v), y(u,v), z(u,v)$ denote the semialgebraic functions that give us the x,y,z coordinates of the point $f(u,v)$, respectively. To parametrize C, it suffices to parametrize the graphs of the functions $x(u,v), y(u,v), z(u,v)$.

Wlog consider $X = \{(u, v, x(u,v) : (u,v) \in (0,1)^2\}$, i.e. the graph of the function $x(u,v)$. Let $p_1(x_1,x_2,x_3) = 0, q_1(x_1,x_2,x_3) > 0, \ldots, q_m(x_1,x_2,x_3) > 0$ be the constraints defining X. We proceed in the same way as in the proof of Lemma 25. Vieweing $p_1, q_1, \ldots, q_m$ as polynomials in x_3, we factorize to obtain

$$\begin{cases} p_1(x_1,x_2,x_3) = (x_3 - h_1^0(x_1,x_2)) \cdot \ldots \cdot (x_3 - h_{\kappa(0)}^0(x_1,x_2)) = 0 \\ q_1(x_1,x_2,x_3) = (x_3 - h_1^1(x_1,x_2)) \cdot \ldots \cdot (x_3 - h_{\kappa(1)}^1(x_1,x_2)) > 0 \\ \cdots \\ q_m(x_1,x_2,x_3) = (x_3 - h_1^m(x_1,x_2)) \cdot \ldots \cdot (x_3 - h_{\kappa(m)}^m(x_1,x_2)) > 0 \end{cases}$$

where each h_r^i is algebraic over $\mathbb{Q}(x_1,x_2)$. We then compute $\kappa(0)$ semialgebraic subsets $S_1, \ldots, S_{\kappa(0)}$ of $\mathbb{R}^2$ that have the following properties.

1. $\bigcup_{j=1}^{\kappa(0)} S_j = (0,1)^2$;
2. For $1 \le j \le \kappa(0)$, the value of x_3 for each $(x_1,x_2) \in S_j$ is equal to $h_j^0(x_1,x_2)$, the jth root of p_1.

This will allow us to write

$$X = \bigcup_{j=1}^{\kappa(0)} \{(x_1, x_2, h_j^0(x_1,x_2)) : (x_1,x_2) \in S_j\}.$$

Now it only remains to observe that the unit square and, by Lemma 26, each S_j can be parametrized using two parameters and algebraic functions.

C Additional Material for Section 4.2

▶ **Lemma 15.** *Given algebraic functions λ, γ, θ in parameter x, with λ not a root of unity, then there is a bound on $n \in \mathbb{N}$ such that there exists an $s \in \overline{\mathbb{Q}}$ with $n = \theta(s)$ and $\lambda^n(s) = \gamma(s)$.*

Proof. If $\theta(x)$ is constant, then n is uniquely determined. If not, by applying heights we get that $\log(n) = h(n) = h(\theta(x))$ and by Lemma 5 we get $a_1, a_2, a_3, a_4 > 0$ such that

$$a_1 h(x) - a_2 \leq h(\theta(x)) = \log(n) \leq a_2 h(x) + a_3. \tag{5}$$

Now we split into the cases where λ is constant or not.

If λ is constant, then there exists fixed $b = h(\lambda)$, such that $h(\lambda^n) = nh(\lambda) = bn$.

Requiring that $\lambda^n = \gamma(x)$ and using Lemma 5 on the algebraic function $\gamma(x)$ we obtain c_3, c_4 such that

$$bn = h(\lambda^n) = h(\gamma(x)) \leq c_3 h(x) + c_4 \tag{6}$$

Combining Equation (6) and Equation (5) we obtain

$$bn \leq c_3 h(x) + c_4 \leq c_3(\log(n) + a_2)/a_1 + c_4,$$

which implies:

$$\begin{aligned}
\sqrt{n} &\leq \frac{n}{\sqrt{n}} \leq \frac{n}{\log(n)} \\
&\leq \frac{1}{b}\left[\frac{c_3}{a_1} + \frac{c_3 a_2/a_1 + c_4}{\log(n)}\right] \\
&\leq \frac{c_3 + c_3 a_2}{b a_1} + \frac{c_4}{b} \qquad \text{if } n \geq 3.
\end{aligned}$$

Thus we bound n:

$$n \leq \max\left\{3, \left(\frac{c_3 + c_3 a_2}{b a_1} + \frac{c_4}{b}\right)^2\right\}.$$

We now consider $\lambda(x)$ not a constant function. Then from Lemma 5 we obtain b_1, b_2, c_3, c_4 such that

$$b_1 h(x) - b_2 \leq h(\lambda(x)) \text{ and } h(\gamma(x)) \leq c_3 h(x) + c_4$$

Using $nh(\lambda(x)) = h(\lambda^n(x)) = h(\gamma(x))$ we obtain $n(b_1 h(x) - b_2) \leq c_3 h(x) + c_4$ which bounds $h(x)$:

$$h(x) \leq \frac{nb_2 + c_4}{nb_1 - c_3} \leq \frac{2b_2 + 2c_4}{b_1} \text{ if } n \geq \max\left\{\frac{2c_3}{b_1}, 1\right\}.$$

Finally we bound n using Equation (5):

$$\log(n) \leq a_3 h(x) + a_4 \leq a_3\left(\frac{2b_2 + 2c_4}{b_1}\right) + a_4.$$

Taken together we have

$$n \leq \max\left\{\frac{2c_3}{b_1}, 1, \exp\left(\frac{a_3(2b_2 + 2c_4) + a_4 b_1}{b_1}\right)\right\}.$$ ◀

Let us now deal with the case where $d_i > 1$ and $\lambda_i = 1$. The equations formed by the constraints of $\begin{pmatrix} 1 & 1 & & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}^n \begin{pmatrix} \tilde{u}_{i,d_i} \\ \vdots \\ \tilde{u}_{i,1} \end{pmatrix} = \begin{pmatrix} \tilde{v}_{i,d_i} \\ \vdots \\ \tilde{v}_{i,1} \end{pmatrix}$ describe a set of polynomial equations in variable n and coefficients in $\mathbb{K}$:

$$\Big\{\tilde{u}_{i,1}(x) = \tilde{v}_{i,1}(x), \quad \tilde{u}_{i,2}(x) + n\tilde{u}_{i,1}(x) = \tilde{v}_{i,2}(x), \quad \ldots, \quad \sum_{i=1}^{k} \binom{n}{i} \tilde{u}_{i,i}(x) = \tilde{v}_{i,k}(x)\Big\}.$$

Let us consider all such equations formed by J_i such that $\lambda_i = 1$. Clearly $\tilde{u}_{i,1} = \tilde{v}_{i,1}$ identically, or else there are finitely many s such that $\tilde{u}_{i,1}(s) = \tilde{v}_{i,1}(s)$. Hence, the first equation can essentially be dropped. Using the second equation to replace n by $(\tilde{v}_{i,2} - \tilde{u}_{i,2})/\tilde{u}_{i,1}$ in all other such equations gives a collection algebraic function only in x. These functions are either identically zero, or have finitely many solutions. If any one function has finitely many instantiations of x then we only need to check these instantiations.

If all of the resulting functions are identically zero, then the system of equations is equivalent to the single equation $n = \theta(x)$, where $\theta(x) = \frac{\tilde{v}_{i,2}(x) - \tilde{u}_{i,2}(x)}{\tilde{u}_{i,1}(x)}$. We can first verify whether the range of $\theta(x)$ over x is bounded. If it is, test every integer n in the range (by Proposition 8).

In the remaining case, $\theta(x)$ is unbounded, so there is a solution to $n = \theta(x)$ for every large n. If this is the only equation, we are done (and the answer is YES). Alternatively there is some other constraint, which we can take from the bottom row of some different Jordan block: $\lambda_j(x)^n = \gamma_j(x)$. We can assume λ_j not a root of unity because the only root of unity was 1, for which all of the constrains are encoded in $n = \theta(s)$. We can now apply the following lemma, which places a bound on n when n appears both linearly and as an exponent w.r.t. algebraic functions:

Again we have an instance of Lemma 15 bounding n that need to be checked.

D Additional Material for Section 5

We complete the proof of Lemma 9:

▶ **Lemma 9.** *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$ and* $\operatorname{rank}\langle\lambda_1, \ldots, \lambda_t\rangle \geq 2$. *Given algebraic functions $\gamma_1, \ldots, \gamma_t$ in $\mathbb{K}$, then it is decidable whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that*

$$\lambda_i(s)^n = \gamma_i(s) \qquad \text{for all} \qquad i = 1, \ldots, t. \tag{2}$$

To do this, we prove Lemma 17, and prove the remaining cases of Subsection 5.2.

D.1 Proof of Lemma 17

In this part we complete the proof of Lemma 17. First we recall some notions from algebraic number theory. Most of the results appear in standard text books on the topic such as [**?**], but an accessible account sufficient for our purposes can be found in [**?**]. An *algebraic integer* is an algebraic number with monic minimal polynomial in $\mathbb{Z}[x]$. Let K be a finite extension of $\mathbb{Q}$, and consider the set $\mathcal{O}_K$ of algebraic integers in K. The set $\mathcal{O}_K$ forms a subring of K, the so-called *ring of integers of* K. The ideals of $\mathcal{O}_K$ are finitely generated, and they form a commutative ring. An ideal $P \neq [1], [0]$ (here $[\alpha]$ is the principal ideal generated by α) is called a *prime ideal* if $P = IJ$, for some ideals I, J, implies that either $I = [1]$ or $I = P$. Each ideal $I \neq [0]$ of $\mathcal{O}_K$ can be represented as a product of *prime ideals*: $I = P_1^{k_1} \cdots P_t^{k_t}$, $k_i \geq 0$, and is unique up to the ordering of the prime ideals in the product.

For a prime ideal P we define the *valuation* $\nu_P \colon \mathcal{O}_K \setminus \{0\} \mapsto \mathbb{N}$ as follows: for $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$ and $[\alpha] = P_1^{k_1} \cdots P_t^{k_t}$, where each P_i is a prime ideal, we set $\nu_P(\alpha) = k_i$ if $P = P_i$, and $\nu_P(\alpha) = 0$ if $P \neq P_1, \ldots, P_t$. By convention we set $\nu_P(0) = \infty$. The valuation ν_P can be extended to the whole number field K by noting that if α is not an algebraic integer, then there exists $m \in \mathbb{N}$, $m \geq 1$, such that $m\alpha = \alpha_1$ is an algebraic integer. In this case we define $\nu_P(\alpha) = \nu_P(\alpha_1) - \nu_P(m)$, and it can be shown that this is well-defined (i.e., does not depend on the choice of α_1 and m).

We need the following properties: for α, $\beta \in K$, and P a prime ideal of $\mathcal{O}_K$,

- $\nu_P(\alpha\beta) = \nu_P(\alpha) + \nu_P(\beta)$.
- $\nu_P(\alpha + \beta) \geq \min\{\nu_P(\alpha), \nu_P(\beta)\}$.
- If $\nu_P(\alpha) < \nu_P(\beta)$ then $\nu_P(\alpha + \beta) = \nu_P(\alpha)$.
- If $\alpha \notin \mathcal{O}_K$, then there is a prime ideal P such that $\nu_P(\alpha) \neq 0$. Furthermore, such a prime ideal can be found effectively.

We shall employ a version Baker's theorem as formulated in [**?**]:

▶ **Theorem 27** (Baker and Wüstholz). *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{C} \setminus \{0, 1\}$ be algebraic numbers different from 0 or 1, and let $b_1, \ldots, b_t \in \mathbb{Z}$ be integers. Write $\Lambda = b_1 \log \alpha_1 + \ldots + b_t \log \alpha_t$, where $\log$ is any branch of the complex logarithm function.*

Let $A_1, \ldots A_t$, B be real numbers larger than e such that $h(\alpha_i) \leq A_i$, and $|b_i| \leq B$ for each i. Let further d be the degree of the extension field $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ over $\mathbb{Q}$.

If $\Lambda \neq 0$, then

$$\log|\Lambda| > -(16td)^{2(t+2)} \log A_1 \cdots \log A_t \log B.$$

As a straightforward consequence we have the following

▶ **Corollary 28.** *For algebraic numbers μ and ζ of modulus 1 with μ not a root of unity, we have $|\mu^n - \zeta| > a/n^b$ for all large enough n and for some effectively computable constants $a > 0$ and $b \in \mathbb{N}$ depending on μ and ζ.*

For a proof, see [**?**, Cor. 8 of Extended Version].

We shall also employ a p-adic version of Baker's theorem proved by K. Yu [**?**]. We employ a version which follows from a version stated in the introduction of K. Yu [**?**] (for definitions, we refer to [**?**]):

▶ **Theorem 29.** *Let $\alpha_1, \ldots, \alpha_t$ $(t \geq 1)$ be non-zero algebraic numbers and K be a number field containing $\alpha_1, \ldots, \alpha_t$, with d the degree of the extension. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, lying above the prime number p, by $e_\mathfrak{p}$ the ramification index of $\mathfrak{p}$, and by $f_\mathfrak{p}$ the residue class degree of $\mathfrak{p}$. For $\alpha \in K$. Let $b_1, \ldots, b_t \in \mathbb{Z}$, and assume that $\Xi := \alpha_1^{b_1} \cdots \alpha_t^{b_t} - 1 \neq 0$. Let further $h_j = \max(h(\alpha_j), \log p)$ for $j = 1, \ldots, t$. Let $B = \max\{|b_1|, \ldots, |b_t|, 3\}$. Then*

$$\nu_\mathfrak{p}(\Xi) < 19(20\sqrt{t+1}d)^{2(t+1)} e_\mathfrak{p}^{t-1} \cdot \frac{p^{f_\mathfrak{p}}}{(f_\mathfrak{p} \log p)^2} \log(e^5 td) h_1 \cdots h_t \log B$$

All the above values are effectively computable given the numbers $\alpha_1, \ldots, \alpha_t$. We have a straightforward corollary:

▶ **Corollary 30.** *Let μ and ζ be algebraic numbers of modulus 1 and assume μ is not a root of unity. Let $K = \mathbb{Q}(\mu, \zeta)$ and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\nu_\mathfrak{p}(\mu^n - \zeta) < C \log n$ as $n \to \infty$ for some effectively computable constant C that depends on $\mathfrak{p}$, μ and ζ.*

Proof. We have $\nu_\mathfrak{p}(\mu^n - \zeta) = \nu_\mathfrak{p}(\zeta) + \nu_\mathfrak{p}(\mu^n \zeta^{-1} - 1)$. Since μ is not a root of unity, the height of μ^n increases linearly in n. ◀

We now recall and prove Lemma 17:

▶ **Lemma 17.** *Suppose λ_1, λ_2 are constant, not roots of unity, multiplicatively independent, and that γ_1, γ_2 are non-constant functions. Then the system $\lambda_1^n = \gamma_1(s)$, $\lambda_2^n = \gamma_2(s)$ has only finitely many solutions.*

Proof. Let the minimal polynomials of γ_1 and γ_2 be P_1 and P_2 with $P_i \in \mathbb{Q}[x, y_i]$. Eliminating x from these polynomials we get a non-zero polynomial $P \in \overline{\mathbb{Q}}[y_1, y_2]$. For points $\alpha_1 = \gamma_1(s_0)$ and $\alpha_2 = \gamma_2(s)$ we have $P(\alpha_1, \alpha_2) = 0$. We are interested in those $n \in \mathbb{N}$ for which $P(\lambda_1^n, \lambda_2^n) = 0$. The sequence $(u_n)_{n=0}^{\infty}$, with

$$u_n = P(\lambda_1^n, \lambda_2^n) = \sum_{k,\ell} a_{k,\ell}(\lambda_1^k \lambda_2^\ell)^n, \tag{7}$$

$a_{k,\ell} \in \overline{\mathbb{Q}}$, is a linear recurrence sequence over $\overline{\mathbb{Q}}$. We wish the characterise those n for which $u_n = 0$.

We first consider the case that $|\lambda_1|$ and $|\lambda_2|$ are multiplicatively independent, that is, $|\lambda_1^i \lambda_2^j| \neq 1$ for all $i, j \in \mathbb{Z}$.

▷ Claim 31. If $|\lambda_1|$ and $|\lambda_2|$ are multiplicatively independent, then there exists an effectively computable $n_0 \in \mathbb{N}$ such that $u_n \neq 0$ for $n \geq n_0$.

Proof. There is a unique pair k, ℓ, with $\lambda_1^k \lambda_2^\ell$ dominant in modulus. Then $(u_n)_n$ has a unique dominant characteristic root, and hence there are only finitely many n for which $u_n = 0$. Indeed, $|u_n|$ grows as $|a_{k,\ell}||\lambda_1^k \lambda_2^\ell|^n + o(|\lambda_1^k \lambda_2^\ell|^n)$, and so $u_n \neq 0$ for all $n \geq n_0$ for some n_0. Now n_0 can be clearly computed using the closed form expression (7) of u_n. ◁

In case the assumption of the above lemma holds, the problem becomes decidable using Proposition 8 for $n \leq n_0$.

In the remainder of this section we assume that $|\lambda_1|$ and $|\lambda_2|$ are multiplicatively dependent. In fact, we may assume that $|\lambda_1| = |\lambda_2|$: We have $|\lambda_1|^i = |\lambda_2|^j$ for some $i, j \in \mathbb{Z}$. By considering the equations $(\lambda_1^i)^n = \gamma_1(s)^i$, $(\lambda_2^j)^n = \gamma_2(s)^j$ instead, we may assume that $|\lambda_1| = |\lambda_2|$; let $\alpha = |\lambda_1| = |\lambda_2|$. We shall show that the new system of equations admits finitely many solutions, and hence so will the original system.

▷ Claim 32. If $\alpha \neq 1$, then there exists an effectively computable constant $n_0 \in \mathbb{N}$, such that $u_n \neq 0$ for all $n \geq n_0$.

Proof. We may assume that $\alpha > 1$ by inverting the equations if necessary. Write $P(x, y) = H(x, y) + G(x, y)$ such that H comprises the maximal (total) degree d monomials of P (and is thus homogeneous), and write $\lambda_1 = \alpha u$, $\lambda_2 = \alpha v$, where $|u|, |v| = 1$. Now H factors into complex lines as it is homogeneous: $H(x, y) = \prod_i (a_i x + b_i y)$, $a_i, b_i \in \overline{\mathbb{Q}}$, so that $H(x, y) = 0$ if and only if $a_i x + b_i y = 0$ for some i. We now have

$$|H(\lambda_1^n, \lambda_2^n)| = (\alpha^d)^n |H((u/v)^n, 1)|.$$

We are assuming, in particular, that λ_1/λ_2 is not a root of unity. We have $a_i \lambda_1^n + b_i \lambda_2^n = 0$ for finitely many n and thus $H(\lambda_1^n, \lambda_2^n)$ vanishes only for finitely many n. Clearly if $|b_i/a_i| \neq 1$ (or either a_i or b_i is zero), the term $a_i \lambda_1^n + b_i \lambda_2^n$ does not vanish, and is bounded below in modulus by a constant (for large n). Assume then that b_i/a_i has modulus 1. Then $|a_i \lambda_1^n + b_i \lambda_2^n| = |a_i||(\lambda_1/\lambda_2)^n + b_i/a_i|$. Applying Corollary 28 we have, for all large enough n and for each i, $|a_i||(\lambda_1/\lambda_2)^n + b_i/a_i| > a/n^c$ where a and c are constants depending on γ_1, γ_2, and b_i/a_i. It follows that for all n large enough $|H(u^n, v^n)| > c_2/n^A$ for some computable c_2, A. We deduce that $|P(\lambda_1^n, \lambda_2^n)| = D(\alpha^d)^n/n^A + \mathcal{O}(\alpha^{(d-1)n})$ for some non-zero constant D. Again we have an effectively computable n_0 after which no solution can occur. ◁

Again, we may invoke Proposition 8 to search among the finitely many n which witness a zero in $(u_n)_n$.

Moving along, we consider the case $\alpha = 1$.

▷ Claim 33. Assume that $\alpha = 1$ and λ_1 is an algebraic integer. Then the conclusion of the above lemma holds.

Proof. Since λ_1 is not a root of unity by assumption, λ_1 has a Galois conjugate $\tilde{\lambda} := \lambda_1^{(i)}$ (as in the definition of the height of λ_1) of modulus larger than 1. By taking σ a Galois conjugation in the field extension of $\mathbb{Q}$ with the elements λ_1, λ_2 and the coefficients of the polynomials of P such that $\sigma(\lambda_1) = \tilde{\lambda}$, by relabelling everything under the conjugation, we have an equivalent problem where we assume $|\lambda_1| > 1$. (In particular, $\sigma(u_n) = 0$ if and only if $u_n = 0$.) We may thus conclude as in the previous cases. ◁

To complete the proof of Lemma 17 we assume that that λ_1 has modulus 1 and is not an algebraic integer. In particular, there exists a prime ideal $\mathfrak{p}$, effectively computable, such that $\nu_{\mathfrak{p}}(\lambda_1) \neq 0$. By replacing λ_1 by λ_2 if necessary, we may assume $\nu_{\mathfrak{p}}(\lambda_1) > 0$. Let now $\mathfrak{p}$ be any such prime ideal. Let us write $P(x, y) = x^j R(x, y) + Q(y)$ with $Q(y) = C \prod_i (y - \beta_i)$ and j is maximal, so that $R(x, y)$ contains a monomial not involving x. Consequently

$$\begin{aligned}\nu_{\mathfrak{p}}(\lambda_1^{jn} R(\lambda_1^n, \lambda_2^n)) &= nj\nu_{\mathfrak{p}}(\lambda_1) + \nu_{\mathfrak{p}}(R(\lambda_1^n, \lambda_2^n)) \\ &\geq nj\nu_{\mathfrak{p}}(\lambda_1) - A_1,\end{aligned}$$

where A_1 is a constant, and

$$\nu_{\mathfrak{p}}(Q(\lambda_2^n)) = \nu_{\mathfrak{p}}(C) + \sum_i \nu_{\mathfrak{p}}(\lambda_2^n - \beta_i).$$

In particular, for $n \geq n_0$ with n_0 effectively computable, we have that the second valuation must be proportional to n whenever $P(\lambda_1^n, \lambda_2^n) = 0$. For non-zero β_i, we have by Corollary 30 $\nu_{\mathfrak{p}}(\lambda_2^n - \beta_i) \leq C_i \log n$ for a constant C_i depending on λ_2, β_i, and $\mathfrak{p}$. So if all the β_i are non-zero, we have an upper bound on n for which equality can hold.

We conclude that at least one $\beta_i = 0$. Still, to have valuation proportional to n, we must have $\nu_{\mathfrak{p}}(\lambda_2) \neq 0$ to have arbitrarily large n solving the system. We may repeat this argument for all $\mathfrak{p}$ for which $\nu_{\mathfrak{p}}(\lambda_1) \neq 0$. Either we get an effective upper bound on n, or $\nu_{\mathfrak{p}}(\lambda_1) \neq 0$ if and only if $\nu_{\mathfrak{p}}(\lambda_2) \neq 0$. We deduce that λ_1 and λ_2 sit over the same prime ideals. Now if $\nu_{\mathfrak{p}}(\lambda_1) = i$ and $\nu_{\mathfrak{p}}(\lambda_2) = j$, consider the equations $\lambda_1^n = \gamma_1(s)$, $(\lambda_2^i/\lambda_1^j)^n = \gamma_2^i/\gamma_1^j(s)$ instead. Now $\nu_{\mathfrak{p}}(\lambda_2^i/\lambda_1^j) = 0$, while $\nu_{\mathfrak{p}}(\lambda_1) = i$, so that the above argument gives an effective bound on n.

This concludes the proof. ◀

D.2 Remaining cases of Subsection 5.2

We first prove Lemma 20:

▶ **Lemma 20.** *Assume that $\{\lambda_1, \ldots, \lambda_t\}$ is multiplicatively dependent modulo constants, but is multiplicatively independent. Then there exists a computable constant n_0 such that system* (2) *admits no solutions for $n > n_0$.*

We need an auxiliary lemma for this.

▶ **Lemma 34.** *Consider the equation $\lambda(s)^n = \gamma(s)$, where neither λ nor γ is constant, and let (n, s) be a solution to it. Then either $n \leq n_0$ or $h(s) < C$ for some constants n_0, C, depending on λ and γ.*

Proof. Recall from Lemma 5 that we have

$$a_1 h(s) - a_2 \leq h(\gamma(s)) \leq a_3 h(s) + a_4 \quad \text{and} \quad b_1 h(s) - b_2 \leq h(\lambda(s)) \leq b_3 h(s) + b_4$$

for some effectively computable constants $a_i, b_i > 0$. Let $n_0 = a_3/b_1$, and assume that $h(s) > \max\{a_2/a_1, b_2/b_1\}$ and $n > n_0$. Then $h(\lambda(s)) \geq a_1 h(s) - a_2 > 0$ and thus

$$n(b_1 h(s) - b_2) \leq h(\lambda(s)^n) = h(\gamma(s)) \leq a_3 h(s) + a_4.$$

It follows that $h(s) \leq \frac{nb_2 + a_4}{nb_1 - a_3}$ which is bounded above by a constant (as a decreasing function with limit b_2/b_1). The claim follows. ◀

Proof of Lemma 20. Assume that $\lambda_1^{a_1} \cdots \lambda_t^{a_t} = c$ identically for some $c \in \overline{\mathbb{Q}}$. Then c is not a root of unity, as otherwise $\{\lambda_1, \ldots, \lambda_t\}$ would not be multiplicatively independent. We obtain the equation

$$c^n = \gamma_1^{a_1} \cdots \gamma_t^{a_t}(s). \tag{8}$$

If the right-hand-side is also a constant, then there is only one n for which the equation can hold ($c^n = c^m = d$ implies $c^{n-m} = 1$), and this n can be effectively computed as an instance of the one-dimensional Kannan–Lipton Orbit Problem.

If it is not constant, then system (2) contains the equation (after relabelling) $\lambda_1(s)^n = \gamma_1(s)$ with γ_1 non-constant. Since at least one of the λ_j is non-constant, we may assume that both λ_1 and γ_1 are non-constant by considering $(\lambda_1\lambda_2(s))^n = \gamma_1\gamma_2(s)$, where λ_2 is non-constant, if necessary. For any solution (n, s), we have by Lemma 34 either $n \leq n_0$ or $h(s) < C_i$ for some constant $n_0 \in \mathbb{N}$, $C_i > 0$. Assuming that $n > n_0$ holds we have the latter bound. Now there exists a constant C such that $h(\gamma_i(s)) < C$ regardless of whether γ_i is constant or not, applying Lemma 5. Consequently, taking heights on both sides of (8), we see that $nh(c) = \sum_{i=1}^t |a_i| h(\gamma_i(s)) < t \max_i\{|a_i|\} C$. It is evident that n is effectively bounded above, and the claim follows. ◀

The remaining cases left from Subsection 5.2 to consider are when λ_1, λ_2, γ_1, γ_2 are multiplicatively dependent, while λ_1 and λ_2 are multiplicatively independent modulo constants. The proof goes along the proof of Lemma 21.

▶ **Lemma 35.** *Assume that λ_1, λ_2, γ_1, γ_2 are multiplicatively dependent, while λ_1, λ_2 are multiplicatively independent modulo constants. Then there exists a computable constant n_0 such that system* (2) *admits no solutions for $n > n_0$.*

Proof. Now any multiplicative relation must involve some γ_i, and without loss of generality $\gamma_2^a = \lambda_1^{a_1}\lambda_2^{a_2}\gamma_1^{a_3}$ with $a \neq 0$. Let us set $c = a_3$ if $a_3 \neq 0$ and $c = 1$ otherwise. We then have the equations

$$\lambda_1(s)^{nc} = \gamma_1(s)^c \quad \text{and} \quad \lambda_2(s)^{na} = \gamma_2(s)^a = \lambda_1(s)^{a_1}\lambda_2(s)^{a_2}\gamma_1(s)^{a_3}.$$

(I.e., if $a_3 = 0$ we keep $\lambda_1(s)^n = \gamma_1(s)$).

Consider the family of pairs of multiplicative relations $\vec{a}_n := (nc, 0, -c)$ and $\vec{b}_n = (-a_1, na - a_2, -a3)$. Clearly, if the $\vec{a}_n$ and $\vec{b}_n$ are collinear, then $n = a/a_2$. So, save for this exceptional n, the the multiplicative relations $\vec{a}_n$ and $\vec{b}_n$ are independent for any $n \geq 1$. (For the claim, we note we can take $n_0 \geq a_2/a$.)

Assume first that λ_1, λ_2, γ_1 are multiplicatively independent. Consider the curve $\mathcal{C}$ defined by these functions (similar to the construction in the proof of Lemma 21), and let $\mathcal{C}'$ be an absolutely irreducible component of it. If the functions are multiplicatively independent modulo constants, we conclude, as in the first part of the proof of Lemma 21, utilising Theorem 18 for all $n \neq a_2/a$.

If the functions are multiplicatively dependent modulo constants, we may apply Theorem 19 as in the second part of the the proof of Lemma 21.

We are left with the case that λ_1, λ_2 and γ_1 are multiplicatively dependent and we have $\gamma_1^b = \lambda_1^{b_1}\lambda_2^{b_2}$ with $b \neq 0$. We again get the equations

$$\lambda_1(s)^{ncb} = \gamma_1(s)^{cb} = \lambda_1(s)^{b_1 c}\lambda_2(s)^{b_2 c} \quad \text{and} \quad \begin{aligned} \lambda_2(s)^{nab} &= \lambda_1(s)^{ba_1}\lambda_2(s)^{ba_2}\gamma_1(s)^{ba_3} \\ &= \lambda_1(s)^{ba_1+a_3b_1}\lambda_2(s)^{a_2b+b_2a_3}. \end{aligned}$$

Recall now that λ_1 and λ_2 are multiplicatively independent. Putting all on one side, we get the equations

$$1 = \lambda_1(s)^{ncb-b_1c}\lambda_2(s)^{-b_2c} \quad \text{and} \quad 1 = \lambda_1(s)^{-ba_1-a_3b_1}\lambda_2(s)^{nab-a_2b}.$$

Notice that now neither cb nor ab equals 0 according to our choices. Let now $\vec{a}_n = (ncb - b_1c, -b_2c)$ and $\vec{b}_n = (-ba_1 - a_3b_1, nab - a_2b)$. The matrix with rows $\vec{a}_n$ and $\vec{b}_n$ has determinant quadratic in n. Hence there are at most two exceptional values of n for which the vectors are collinear. Otherwise $\vec{a}_n$ and $\vec{b}_n$ are $\mathbb{Z}$-linearly independent. It is evident that, save for the at most two exceptional values of n, the multiplicative relations $\vec{a}_n$ and $\vec{b}_n$ are $\mathbb{Z}$-linearly independent. Hence for n not an exceptional value, there are finitely many points s for which the equations can be satisfied. (Again, for the claim, we may take n_0 larger than both of the two exceptional values of n.) On the other hand, we may solve the problem for the exceptional values of n using Proposition 8.

Consider again the curve defined by λ_1 and λ_2 similar to the above, and any of its absolutely irreducible components. As λ_1 and λ_2 are multiplicatively independent modulo constants, we may apply Theorem 18 to conclude as above. This concludes the proof. ◀

E Additional Material for Section 6

E.1 W.l.o.g. there is a single equation

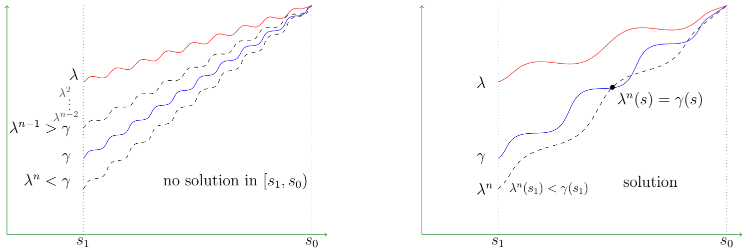

Figure 1 Cases for $\lambda(s) \to 1$ as $s \to s_0$.

▶ **Lemma 22.** *Suppose* $\operatorname{rank}\langle\lambda_1, \ldots, \lambda_t\rangle = 1$, *then whether there is a solution* $(n, s) \in \mathbb{N}\times\mathbb{R}\setminus\mathcal{E}$ *to* $\lambda_i^n(s) = \gamma_i(s)$ *for all* $i = 1, \ldots, t$ *reduces to instances with* $t = 1$.

Proof. Recall that when $\operatorname{rank}\{\lambda_1, \ldots, \lambda_t\} = 1$, we may replace the system of equations with a system consisting of one equation $\lambda(s)^n = \gamma(s)$. The process might involve creating new solutions that do not solve the original system. We take care of this problem by showing how to recover solutions to the main system from solutions to the single equation system.

Assume first that there exists a non constant eigenvalue λ attaining non-real values. Then, by assumption, also its complex conjugate $\overline{\lambda}$ is an eigenvalue. As $\operatorname{rank}\{\lambda, \overline{\lambda}\} = 1$, we have $\lambda^a = \overline{\lambda}^b$ with a, b non-zero since neither is assumed to be a root of unity. If $a = 1, b = -1$ (or visa-versa) then $\lambda = (\overline{\lambda})^{-1}$, hence $|\lambda| = \frac{1}{|\lambda|}$, thus $|\lambda| = 1$.

If $a = b$ then $\lambda^a = \overline{\lambda}^a = \overline{\lambda^a}$, thus λ^a is real (and so λ^{2a} is positive and real). This case was eliminated already by Lemma 13.

In the remaining $a \neq b$ and $|a| > 1$: we get $\lambda^{b+a} = |\lambda|^{2b}$, and taking absolute values both sides, we get $|\lambda|^{b+a} = |\lambda|^{2b}$, which occurs only when $|\lambda| = 1$ identically. Therefore the values of λ lie on the unit circle.

Assume that the system contains also a real-valued function λ_1. We similarly have $\lambda_1^c = \lambda^d$ with c and d not zero. Taking again absolute values on both sides, we have that $|\lambda_1|^c = 1$. It follows that $\lambda_1 = \pm 1$, and we therefore have λ_1 is a constant root of unity. But, we may remove such an eigenvalue from the analysis by Lemma 16. We may thus assume that either all eigenvalues are real-valued, or are complex-valued with values on the unit circle.

Assume first that all the eigenvalues of the system are real-valued (and not constant ± 1). We show that we may assume there exists a function μ, not necessarily any one of the eigenvalues, such that $\lambda_i = \mu^{b_i}$ for each i. If there is only one such eigenvalue, there is nothing to prove, so assume that there are several. Partition the domain in intervals such that in each interval, the λ_i and γ_i have constant sign. We first show that we may assume they are both positive. Indeed, if in any interval we have λ_i positive and γ_i negative, there can be no solutions. If λ_i is negative and γ_i is positive, then there can only be solutions with n even. Therefore, we may replace the equations by $\lambda_i^2(s)^{n_1} = \gamma_i(s)$, with $n_1 \in \mathbb{N}$ without creating spurious solutions. Here both $\lambda_1^2(s)$ and γ_i are positive. Similarly, if both λ_i and γ_i are negative, there can only be a solution for odd n. We may therefore replace the equations with $\lambda_i^2(s)^{n_1} = \gamma_i/\lambda_i(s)$, where $n_1 \in \mathbb{N}$. No new solutions are created in this process, while λ_1^2 and γ/λ are both positive.

We may from now on consider one of the finitely many intervals in the above partition. For each pair λ_1, λ_2, we have $\lambda_1^{a_i} = \lambda_i^{b_i}$ for some non-zero a_i and b_i. Recall that we also have $\gamma_1^{a_i} = \gamma_i^{b_i}$ by assumption (otherwise $\gamma_1^{a_i}(s) = \gamma_2^{b_i}(s)$ holds for at most finitely many s, deeming the problem decidable). Take $\mu = \lambda_1^{1/\ell}$ and $\eta = \gamma_1^{1/\ell}$ where $\ell = \operatorname{lcm}_i(b_i)$. This is well-defined as the λ_i and γ_i are positive. Then for each i we have $\lambda_i = \lambda_1^{a_i/b_i} = \mu^{\ell_i}$ and similarly $\gamma_i = \eta^{\ell_i}$, for some integer ℓ_i. Now any solution of $\mu^n(s) = \eta(s)$ is a solution to the whole system, and it thus suffices to search for solutions for this single equation.

We then turn our attention to the case of eigenvalues attaining non-real values. As pointed out above, the values of the eigenvalues lie on the unit circle. Assume that λ_1 is such. Recall that for each λ_i we have non-zero a_i, $b_i \in \mathbb{Z}$ such that $\lambda_1^{a_i} = \lambda_i^{b_i}$ and $\gamma_1^{a_i} = \gamma_i^{b_i}$. Partition the domain into many finitely intervals according to the points where the non-constant $\lambda_1^{a_i}$, $\lambda_i^{b_i}$, $\gamma_1^{a_i}$, and $\gamma_i^{b_i}$ attain the value -1. (If some γ_i is constant -1 we do not take this into consideration when defining the intervals. Also, by assumption none of the λ_i are constant -1 as this is a root of unity). Let Log be the principal branch of the complex logarithm function, and for $a \in \mathbb{N}$, $a \geq 1$, define $z^{1/a} := \exp(1/a \operatorname{Log} z)$. Notice that the function is not continuous for $z \in \mathbb{C}$, but in each of the intervals constructed above, the functions $\lambda_i^{1/a}$ are continuous and single-valued. We focus on one of the intervals from now on. We show that there exist algebraic functions μ, η, integers ℓ_i, and b_ith roots of unity ω_i, ω_i' such that $\lambda_i = \omega_i \mu^{\ell_i}$ and $\gamma_i = \omega_i' \eta^{\ell_i}$ for each i. Let $\ell = \operatorname{lcm}_i(b_i)$ and set $\mu = \lambda_1^{1/\ell}$ and $\eta = \gamma_1^{1/\ell}$. Then $\lambda_1 = \mu^\ell$, $\gamma_1 = \eta^\ell$, and $\mu^{\ell a_i} = \lambda_1^{a_i} = \lambda_i^{b_i}$. Similarly $\eta^{\ell a_i} = \gamma_i^{\ell_i}$. It follows that $\lambda_1 = \omega_i \mu^{\ell_i}$ for some ω_i a b_ith root of unity, and $\ell_i = a_i \ell / b_i \in \mathbb{Z}$. Indeed, for any s we have $\lambda_i(s) = \omega_s \mu^{\ell_i}(s)$

for some b_ith root of unity ω_s. By continuity, ω_s is also continuous, and hence is constant. Similarly $\gamma_i = \omega_i' \eta^{\ell_i}$, as desired.

The equations are now equivalent to

$$(\omega_i \mu^{\ell_i}(s))^n = \omega_i' \eta^{\ell_i}(s) \qquad i = 1, \ldots, t.$$

Considering the subsequences $n = r\ell + m$, $r \in \mathbb{N}$, for $m = 0, \ldots, \ell - 1$, we may consider the equations

$$\mu^{\ell_i}(s)^n = \omega_i'' \eta^{\ell_i}(s), \qquad i = 1, \ldots, t,$$

where ω_i'/ω_i^m has been combined into ω_i'', yet another b_ith root of unity, with $\omega_1'' = 1$.

The solutions to $\lambda_1(s)^n = \gamma_1(s)$ are in one-to-one correspondence to the union of the solutions to $\mu(s)^n = \omega\eta(s)$ where ω ranges over the ℓth roots of unity. Assuming (n, s) is a solution to $\mu(s)^n = \omega\eta(s)$, we get $\mu^{\ell_i}(s)^n = \omega^{\ell_i}\eta^{\ell_i}(s)$ for each i. We thus deduce that the system of equations has a solution if and only if $\mu(s)^n = \omega\eta(s)$ for some ℓth root of unity ω such that $\omega^{\ell_i} = \omega_i''$ for each $i = 2, \ldots, t$. It is plain to check whether the ω_i'' satisfy such a relation, so it suffices to characterise the solutions to $\mu(s)^n = \omega\eta(s)$, ω any one of the ℓth roots of unity. ◀

E.2 Real case

▶ **Lemma 23.** *Given real algebraic functions λ and γ, it is decidable whether there exists $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda^n(s) = \gamma(s)$.*

Proof. For real-valued functions f, g, if $f(x) < g(x)$ for all x in a set E, we use the notation $f < g$ (over E).

Let us consider the partition of $\mathbb{R} \setminus \mathcal{E}$ into interval subsets $S_1, \ldots, S_i$, such that for each subset either $0 \le |\lambda| < 1$, or $|\lambda| > 1$, with the finite set of points $\{s : \lambda(s) = 1\}$ excluded and handled separately (recall, by Lemma 13 and Lemma 16 λ is not constant 0 or 1). We will focus on the subsets where $|\lambda| \le 1$. Given such a subset S_i, we only need to consider each interval $D \subseteq S_i$ where $\{s \mid 0 \le |\gamma(s)| \le 1\}$. The remaining case where $|\lambda| > 1$ reduces to our case by considering $\frac{1}{\lambda^n}(x) = \frac{1}{\gamma}(x)$. Note that this partition is finite as the function $|\lambda(x)| = 1$ at only finitely many points (similarly for $|\gamma(x)| = 1$), and these points can be checked explicitly.

First let us consider λ constant, and we may assume $0 < \lambda < 1$. Then compute $a = \inf_x \gamma_i(x)$ and $b = \sup_x \gamma_i(x)$ and decide whether there exists n such that $a \le \lambda_i^n \le b$. Henceforth, λ is not constant.

Whilst we assume $|\lambda(x)| < 1$, still $|\lambda(x)|$ could be arbitrarily close to 1. We first consider the subset of D where this is not the case. Let $\delta > 0$ be a small rational number, and consider the set $\mathcal{S}_\lambda(\delta) \subseteq D$ comprising those s such that $|\lambda(x)| < 1 - \delta$. Then, for each $s \in \mathcal{S}_\lambda(\delta)$ we have $|\lambda^n(x)| < (1-\delta)^n$ for all $n \ge 0$. In particular, $\lambda^n(s)$ tends to 0 exponentially.

Similary bounding $|\gamma|$ away from 0, let $\mathcal{S}_\gamma'(\delta')$, for $\delta' > 0$ a small rational number, comprise those points $s \in \mathcal{S}_\lambda(\delta)$ for which $|\gamma(s)| > \delta'$.

Then, for n larger than $\log(\delta')/\log(1-\delta)$, we have $|\lambda^n| < |\gamma|$, leading to the lemma:

▶ **Lemma 36.** *Let $\delta, \delta' > 0$ be fixed small rational numbers. Then there exists $n_{\delta,\delta'} \in \mathbb{N}$ such $\lambda^n(s) = \gamma(s)$ does not have a solution with $n \ge n_{\delta,\delta'}$ and $s \in \mathcal{S}_{\lambda,\gamma}(\delta, \delta') = \mathcal{S}_\gamma'(\delta') \cap \mathcal{S}_\lambda(\delta)$.*

Hence, given δ, δ' and having computed $n_{\delta,\delta'}$, solutions for each $n \le n_{\delta,\delta'}$ can be found by Proposition 8.

Recall, without loss of generality we assume λ, γ are positive, if necessary by taking even or odd sub-sequences. Hence the remaining cases for $s \in D \setminus \mathcal{S}'_\gamma(\delta')$, that is when $\lambda(s)$ is approaching 1, or $\gamma(s)$ is approaching 0.

We will make repeated use of the following immediate consequence of the intermediate value theorem

▶ **Lemma 37.** *Given two continuous functions f, g on the interval $[a, b]$ with $f(a) < g(a)$ and $f(b) > g(b)$, there exists s such that $f(s) = g(s)$.*

and its immediate corollary:

▶ **Corollary 38.** *Given two continuous functions f, g on the interval (a, b). One of the following occurs*

- *$f(x) > g(x)$ for all $x \in (a, b)$, or*
- *$f(x) < g(x)$ for all $x \in (a, b)$, or*
- *there exists $s \in (a, b)$ such that $f(s) = g(s)$*

Proof. Suppose there exists $x, y \in (a, b)$ such that $f(x) > g(x)$ and $f(y) < g(y)$, then on the interval $[x, y] \subseteq (a, b)$ there exists s such that $f(s) = g(s)$. ◀

We assume that δ, δ' are chosen giving interval $D \setminus \mathcal{S}_{\lambda,\gamma}(\delta, \delta')$. Let E be one such interval with problematic endpoint s_0, that is $E = (s_0, s_1]$ or $E = [s_1, s_0)$. We assume we choose δ, δ' small enough so that $\lambda(x)$ and $\gamma(x)$ are monotonic in E. This is because the derivative of an algebraic function is an algebraic function[5], and therefore has finitely many roots, thus the function changes direction finitely many times. Furthermore, it is evident that such δ, δ' are effectively computable.

Let us start with the case that $\lambda(x) \to 1$ as $x \to s_0$.

First, let us assume there exists b_1, b_2 such that $0 < b_1 < \gamma < b_2 < 1$ over E, then since $\lambda(s_1) < 1$ we have $\lambda(s_1)^n < b_1$ for some n (and $\lambda(x)^n \to 1 > b_2$ as $x \to s_0$). Hence by Lemma 37, there is a solution $\lambda^n(s) = \gamma(s)$ at some point $s \in E$. Clearly n is computable, and we may compute a suitable s for which equality holds.

Otherwise we have $\gamma(x)$ is also approaching 1 or 0 as $x \to s_0$. Let us start with 1: It must be the case, by Corollary 38, that either $\gamma < \lambda$ or $\lambda < \gamma$ in E, otherwise there is a point s such that $\lambda(s) = \gamma(s)$ and the answer is YES (in fact, at $n = 1$). If $\lambda < \gamma$ then the answer is NO, as $\lambda^n < \lambda < \gamma$ over E. Hence we must consider $\lambda > \gamma$ and so $1 > \lambda(s_1) > \gamma(s_1)$.

Then we can compute n such that $\lambda(s_1)^n < \gamma(s_1)$. After this occurs either there exists s such that $\lambda(s)^n = \gamma(s)$, or $\lambda^n < \gamma$ and so we only need to check every $m \leq n$ (via, Proposition 8). These two cases are depicted in Figure 1.

Now let us assume $\gamma(x) \to 0$ as $x \to s_0$. Similarly we assume monotonicity of λ, γ as $x \to s_0$. Again we have $\lambda > \gamma$ over E (otherwise $\lambda(s) = \gamma(s)$ at some s, answer YES, or $\lambda^n < \lambda < \gamma$, answer NO). Again we search for n such that $\lambda(s_1)^n < \gamma(s_1)$, at which point either there exists s such that $\lambda(s)^n = \gamma(s)$ or $\lambda^n < \gamma$ over E and hence $\lambda^m < \gamma$ for all $m \geq n$ (it remains to check each $1, \ldots, n$ manually, via Proposition 8). ◀

[5] Differentiating the polynomial defining λ implicitly with respect to x, we get a polynomial $P(s, \lambda(x), \lambda'(x))$. Eliminating with respect to $\lambda(x)$, we get a polynomial relation with s and $\lambda'(x)$

E.3 Non-real case

We prove

▶ **Lemma 24.** *Let λ and γ be algebraic functions. Assume λ is not real, non-zero, not a root of unity, and of modulus 1. The equation $\lambda(s)^n = \gamma(s)$ admits solutions as follows. If γ is not of modulus* 1 *constantly, then there are finitely many s. If γ is of modulus 1 identically and λ is constant, then there are infinitely many solutions and such a solution can be effectively found. Finally, if λ is not constant, then the equation admits a solution for all $n \geq n_0$, and n_0 is computable.*

Proof of Lemma 24. Since λ is of constant modulus 1, we are only concerned with points where γ is of modulus 1. If γ is not of constant modulus 1, then there are only finitely many s for which γ intersects the unit circle and only these points need to be checked

Assume first that λ is a constant. If γ is of constant modulus 1, then the range of γ defines (possible several) open arcs on the unit circle. The orbit of λ is dense on the unit circle, as it is not assumed to be a root of unity. Therefore, there exist (infinitely many) integers n such that λ^n hits such an arc. Such an n can be straightforwardly computed, after which the suitable s can be computed. The single equation therefore always has a solution.

Otherwise, we may assume that λ and γ define continuous arcs on the circle. Furthermore, we may assume that the arcs do not cross the line $(-\infty, 0]$. (In case γ is constant, it defines a point.) Let us write λ and γ in polar form: $\lambda = \exp(\mathrm{i}\theta)$, $\gamma = \exp(\mathrm{i}\psi))$, where now $\theta, \psi \colon D \to [-\pi, \pi)$ are continuous, and i is the imaginary unit. The derivative of an algebraic function is algebraic, here it is $\mathrm{i}\theta'(x)\exp(\mathrm{i}\theta(x))$. We deduce that $\theta'(x)$ is an algebraic function, and the zeros of it may be computed. We may define an interval in which θ and ψ are monotone: they draw continuous arcs on the unit circle and are rotating in one direction with s varying. Compute some approximations θ_0, ψ_0 of the length of the arcs, and compute n so large, so that $n\theta_0 > 4\pi + \psi_0$ (notice that the $n\theta_0$ gives an approximation for the length of the arc defined by λ^n). So, while s ranges over the interval, the arc of λ^n winds around the unit circle at least twice. By the intermediate value theorem there must be a point at which $\lambda^n(s) = \gamma(s)$. To see this, map the progress of the arc onto the real line. Let the endpoints of the interval be s_0 and s_1. Assume $\theta(s_0) < \psi(s_0) \leq \theta(s_0) + 2\pi$ (if not, add integer multiples of 2π to $\psi(s_0)$). Now $n\theta(s_1) \geq \theta(s_0) + 4\pi \geq \psi(s_0) + 2\pi > \psi(s_1)$. Consequently, by the intermediate value theorem, there must be a point where the values $n\theta$ and ψ coincide, as they are continuous functions. ◀