The Orbit Problem for Parametric Linear Dynamical Systems

Christel Baier*, Florian Funke*, Simon Jantsch*, Engel Lefaucheux†, Florian Luca‡†§,
Joël Ouaknine†, David Purser†, Markus A. Whiteland† and James Worrell¶
*Technische Universität Dresden, Germany
†Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany
‡School of Mathematics, Wits University, Johannesburg, South Africa
§Research Group in Algebraic Structures and Applications, King Abdulaziz University, Jeddah, Saudi Arabia
¶Department of Computer Science, 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 four or more parameters.**

More precisely, consider a d-dimensional square matrix M whose entries are rational functions in one or more real variables. Given initial and target vectors $u, v \in \mathbb{Q}^d$, the parametrised 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 in the case where 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 four or more parameters.

***Index Terms*—Orbit problem, parametric, linear dynamical systems.**

I. 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 [1] over ten years after Harrison first raised the question of decidability [2]. 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 (see the references in Section I-A).

Formally, the *Parametric Orbit Problem* is as follows: given a matrix $M \in \mathbb{Q}(\vec{x})^{d\times d}$ whose entries are rational functions in ℓ real variables $\vec{x} = (x_1, ..., x_\ell)$, initial and target vectors $u, v \in \mathbb{Q}^d$, do there exist $\vec{s} \in \mathbb{R}^\ell$, i.e., values of the parameters giving rise to a concrete matrix $M(\vec{s}) \in \mathbb{R}^{d\times d}$, and a positive integer $n \in \mathbb{N}$, such that $M(\vec{s})^n u = v$?

We prove two main results in this paper. In the case of four or more parameters 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. In the case of a single parameter we show that the Parametric Orbit Problem is decidable. In fact, in this case we also allow the source and target vectors u, v to have entries that are rational functions over the parameter. Thus our main theorem is as follows:

Theorem I.1. *It is decidable, given a parametric matrix $M \in \mathbb{Q}(x)^{d\times d}$ depending on a single parameter x, and parametric initial vector $u \in \mathbb{Q}(x)^d$ and target vector $v \in \mathbb{Q}(x)^d$, whether there exist $s \in \mathbb{R}$ and an integer $n \in \mathbb{N}$ such that $M(s)^n u(s) = v(s)$.*

Theorem I.1 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 I.1 follows a case distinction based on properties of the eigenvectors of the matrix M (which are algebraic functions) and the shape of the Jordan normal form J of M. 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 $1 \le i \le t$, 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 Eq. (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 [3, Theorem 2] and [4]) 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 Eq. (1) geometrically in terms of whether a curve

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

intersects the multiplicative group

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

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 $\lambda_1, \dots, \lambda_t$ and $\gamma_1, \dots, \gamma_t$.

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 $\lambda_1, \dots, \lambda_t$ has rank one, we provide in Section VI a direct elementary method to find solutions of the Eq. (1).

Another main case in the proof of Theorem I.1 is when matrix J has a Jordan block of size at least 2, i.e., it is not diagonal (see Section IV-C). Similar to the situation with the original Orbit Problem, this case is more straightforward. 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 smallest $n \in \mathbb{N}$ such that the equation $M(s)^n u(s) = v(s)$ in Theorem I.1 admits a solution $s \in \mathbb{R}$.

A. Related work

Reachability problems in (unparametrized) linear dynamical systems have a rich history. Answering a question by Harrison [2], Kannan and Lipton [1] 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 [5]. This was extended to polytope targets in [6], and later further generalized to polytope initial sets in [7]. Orbit problems have recently been studied in the setting of rounding functions [8].

If the parametric matrix M is the transition matrix of a parametric Markov chain (pMC) [9]–[11], 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 [12]. An important problem in this direction is to find parameter settings with prescribed properties [13]–[15], which has also been studied in the context of model repair [16], [17]. While all previous references use the standard path-based semantics of Markov chains, the distribution transformer semantics [18]–[20] 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.

Decidability of the Skolem Problem is known for matrices of dimension at most four [21], [22]. A continuous version of the Skolem Problem was examined in [23]. With the prolonged intractability of the Skolem Problem in general, it has recently been used as a reference point for other decision problems [24]–[26].

Ostafe and Shparlinski [27] consider the Skolem Problem for parametric families of simple linear recurrences. More precisely, they consider linear recurrences of the form $u_n = a_1(s)\lambda_1(s)^n + \dots + a_k(s)\lambda_k^n(s)$ for rational functions $a_1, \dots, a_k, \lambda_1, \dots, \lambda_k$ 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 s 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).

II. Preliminaries

Given a set of variables X, we denote the ring of polynomials over X with base field $\mathbb{Q}$ by $\mathbb{Q}[X]$. The field of fractions, i.e., the rational functions in X, is denoted by $\mathbb{Q}(X)$.

Definition II.1. 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*;
- $M \in \mathbb{Q}(X)^{d \times d}$, the *parametrized matrix*;
- $u \in \mathbb{Q}(X)^d$ an initial distribution.

Given $s \in \mathbb{Q}^{|X|}$, we denote by $M(s)$ the matrix $\mathbb{Q}^{d \times d}$ obtained from M by invoking each rational function in M on the set of parameters 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 $u(s)$: $\{u(s), M(s)u(s), M(s)^2u(s), \dots\}$. $(M(s), u(s))$ *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 $M(x)$ is undefined only at poles of the entries of $M(x)$. For any fixed n, the elements of $M^n(x)$ are polynomial in the entries of $M(x)$, so no new poles are introduced when powering $M(x)$. Consequently, $M^n(x)$ is defined whenever $M(x)$ is.

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

A. 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 [28]–[30] 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, a, ε), where $p \in \mathbb{Q}[x]$ is its minimal polynomial, $a = a_1 + a_2 i$, with $a_1, a_2 \in \mathbb{Q}$, is an approximation of α, and $\varepsilon \in \mathbb{Q}$ is sufficiently small such that α is the unique root of p within distance ε of a (such ε can be computed by the root-separation bound, due to Mignotte [31]). 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.

Given an algebraic number α with (normalised) minimal polynomial

$$a_d x^d + \cdots + a_1 x + a_0 = a_d(x - \alpha^{(1)}) \cdots (x - \alpha^{(d)}) \in \mathbb{Z}[x]$$

where $\alpha^{(1)} = \alpha$ and $a_d \geq 1$, define the *height* $h(\alpha)$ as

$$h(\alpha) = \frac{1}{d}\left(\log a_d + \sum_{i=1}^{d} \log(\max\{|\eta^{(i)}|, 1\})\right).$$

This is called *Weil's absolute logarithmic height*. By convention we set $h(0) = 0$.

For all algebraic numbers a, b, and integers n we have:

(i) $h(a + b) \leq h(a) + h(b) + \log 2$;
(ii) $h(ab) \leq h(a) + h(b)$;
(iii) $h(a^n) = nh(a)$

In addition for $a \neq 0$ we have $h(a) = 0$ if and only if a is a root of unity[1] by a theorem of Kronecker. Given a number field K, that is, a finite (algebraic) extension of $\mathbb{Q}$, the set of $\alpha \in K$ with $h(\alpha)$ bounded above by a constant is finite.

B. Algebraic functions

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 an algebraic function has finitely many zeros and poles, and furthermore, these zeros and poles are algebraic. Indeed, let $P(x, y) = a_d(x)y^d + \cdots + a_1(x)y + a_0(x)$, 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, $y^{-d}P(x, y) = a_d(x) + \ldots + a_1(x)y^{1-d} + a_0(x)y^{-d}$, so that a pole of f is a zero of $a_d(x)$.

Let $P(x, y) = \sum_{i=0}^{d} a_i(x)y^d \in \mathbb{Q}[x, y]$. 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 entries in the field of rational functions $\mathbb{Q}(x)$ with characteristic polynomial $P(x, y) \in \mathbb{Q}(x)[y]$. Write $c_1, \ldots, c_m \in \mathbb{C}$ for the finite set of critical points of the irreducible factors of P. Then there exist a connected open subset $U \subseteq \mathbb{C}$ such that $\mathbb{R}\backslash\{c_1, \ldots, c_m\} \subseteq U$, and d holomorphic[2] functions $\lambda_1, \ldots, \lambda_d : U \to \mathbb{C}$ (not necessarily distinct) such that the characteristic polynomial $P \in \mathbb{Q}(x)[y]$ of M factors as

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

for all points $x \in U$.

Definition II.2. A collection $Y = \{\lambda_1, \ldots, \lambda_t\}$ of algebraic functions defined on a common domain U is said to be *multiplicatively dependent* if there exist $a_1, \ldots, a_t \in \mathbb{Z}$ not all zero, such that $\lambda_1^{a_1} \cdots \lambda_t^{a_t} = 1$ identically away from poles and zeros of $\lambda_1, \ldots, \lambda_t$. Otherwise Y is called *multiplicatively independent*.

The *rank* $\operatorname{rank} Y$ is defined as the size of the largest multiplicatively independent subset of Y.

We say that Y is *multiplicatively dependent modulo constants* if there exist $a_1, \ldots, a_t \in \mathbb{Z}$ not all zero, and a constant $c \in \overline{\mathbb{Q}}$, such that $\lambda_1^{a_1} \cdots \lambda_t^{a_t} = c$ identically away from poles and zeros of $\lambda_1, \ldots, \lambda_t$. Otherwise Y is *multiplicatively independent modulo constants*.

Thus $\operatorname{rank}(\lambda_1, \ldots, \lambda_t)$ is the smallest necessary number of the generators of the multiplicative group generated by $\lambda_1, \ldots, \lambda_t$. For example, if $\operatorname{rank}(\lambda_1, \ldots, \lambda_t) = 1$, 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 [32, Sect. 3.2], Derksen, Jeandel, and Koiran give an algorithm for computing the generators of the groups $\{(a_1, \ldots, a_t) \in \mathbb{Z}^t : \lambda_1^{a_1} \cdots \lambda_t^{a_t} = c \in \overline{\mathbb{Q}}\}$ and $\{(a_1, \ldots, a_t) \in \mathbb{Z}^t : \lambda_1^{a_1} \cdots \lambda_t^{a_t} = 1\}$ for a given set $\{\lambda_1, \ldots, \lambda_t\}$ of non-zero algebraic functions. It is therefore straightforward to compute the rank of the given set using the latter algorithm.

Consider now an algebraic function λ which is not constant. In our analysis, we shall need to bound $h(\lambda(s))$ in terms of $h(s)$, as long as s is not a zero or a pole of λ. 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 [33] shows that $C_P = 5\left(\log\left(2^{\min\{d_x, q\}}(d_x + 1)(d_y + 1)\right) + h_p(P)\right)^{1/2}$ suffices, and hence an upper bound is for C_P is computable, given P. Here $h_p(P)$ is the *height of the polynomial* P. For

[1] z is a root of unity if there exists $k \in \mathbb{N}$ such that $z^k = 1$

[2] holomorphic functions are complex-valued functions complex-differentiable in some neighbourhood of every point of the domain.

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.

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

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

We formulate a corollary sufficient for our needs:

Lemma II.3. *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*

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

III. Multi parameter synthesis for point reachability problem is Skolem-hard

A sequence $(u_n)_{n=1}^{\infty}$ satisfying a recurrence relation of the form $u_n = a_1 u_{n-1} + a_2 u_{n-1} + \cdots + a_k u_{n-k}$ is called a *linear recurrence sequence* (LRS). The *order* of the sequence is the minimal k for which such a recurrence relation exists. The sequence is then uniquely defined by its first k values $u_1, \ldots, u_k$. For an order k LRS we clearly have $a_k \neq 0$. The *Skolem Problem* asks, given an LRS $(u_n)_n$, 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 Skolem reduces to are said to be *Skolem-hard*. We will now reduce the Skolem problem to the parameter synthesis problem.

An order k LRS $u_n = a_1 u_{n-1} + a_2 u_{n-1} + \cdots + a_k u_{n-k}$ with initial terms $\vec{u} = (u_k, \ldots, u_1)$ can be represented in matrix form by $u_{k+n} = (1, 0, ..., 0) A^n \vec{u}^{\top}$, where

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

In matrix form, the Skolem problem asks if the orbit $\{A^n \vec{u} \colon n \geq 0\}$ of $\vec{u}$ under A hits the hyperplane $\{(x_k, \ldots, x_1) \in \mathbb{R}^k \colon x_k = 0\}$. This can be encoded by constant matrix A, initial vector $\vec{u}$ and the parametric target $v(x_1, \ldots, x_{k-1}) = (0, x_1, \ldots, x_{k-1})$. In fact, it is also possible to define the problem with parametric matrix and constant target.

Theorem III.1. *The Multi Parameter Reachability Problem is Skolem-hard, even if the initial and target vectors are constant functions.*

Proof. Let A be a constant matrix representing the behaviour of an LRS $(u_n)_n$, and let $\vec{u} = (u_k, \ldots, u_1)$ be the initial configuration. Notice that matrix A is invertible. Indeed, a matrix is invertible iff it has determinant (the product of its eigenvalues) different from zero. The eigenvalues of this matrix are the roots of its characteristic polynomial $x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_{k-1} x - a_k$, none of which are zero, since $a_k \neq 0$.

Let $B : \mathbb{R}^{k-1} \to \mathbb{R}^{d \times d}$ be a diagonal parametric matrix, over $k-1$ parameters, with diagonal entries $\langle 0, x_1, \ldots, x_{k-1} \rangle$. This is used to describes the target hyperplane $B(x)\vec{1} = \{(0, x_1, \ldots, x_{k-1})^{\top} \mid x_i \in \mathbb{R}\}$.

Let $M(x) = \begin{pmatrix} 0 & 0 \\ A^{-1}B(x) & A^{-1} \end{pmatrix}$, and observe that, for the initial point $\begin{pmatrix} \vec{1} \\ 0 \end{pmatrix}$, we have $M^n \begin{pmatrix} \vec{1} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ (A^{-1})^n B(x)\vec{1} \end{pmatrix}$.

Hence the problem $M(x)^n \begin{pmatrix} \vec{1} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ u \end{pmatrix}$, restricted only to the non-zero dimensions, requires $(A^{-1})^n B(x)\vec{1} = \vec{u}$. Equivalently, we need $A^n \vec{u} = B(x)\vec{1}$, requiring $A^n \vec{u}$ to hit the required hyperplane of the Skolem problem. □

Our proof of Skolem-hardness requires a number of parameters that is 1 minus the order of the LRS. In particular, since Skolem is unsolved at order 5, the Parameter synthesis reachability problem cannot be solved from parameter dimension 4 without advances to the Skolem problem. This motivates our search for low dimensional reachability, in particular single parameter synthesis in the next section.

Remark (Positivity-hardness)**.** Similarly by expressing target $v(x_1, \ldots, x_k) = (x_1^2, x_2, \ldots, x_k)$, we can reduce the *positivity problem*, which asks if there exists $n \in \mathbb{N}$ s.t. $u_n \geq 0$. Similar to the Skolem problem, the positivity problem has been shown to be decidable for linear recurrence sequences of low order [34], but remains notoriously unsolved in general.

IV. Single Parameter Reachability: Overview of proof

In this section we show how to prove to Theorem I.1:

Theorem I.1. *It is decidable, given a parametric matrix $M \in \mathbb{Q}(x)^{d \times d}$ depending on a single parameter x, and parametric initial vector $u \in \mathbb{Q}(x)^d$ and target vector $v \in \mathbb{Q}(x)^d$, whether there exist $s \in \mathbb{R}$ and an integer $n \in \mathbb{N}$ such that $M(s)^n u(s) = v(s)$.*

We will show that either

(i) there exists a finite number of algebraic parameters that may allow the LDS to reach the target, or
(ii) we can bound the number of iterations of the matrix that may be needed.

In the first case, the decidability is a direct consequence of the fact that the choice of parameter leads to a concrete matrix, thus giving an instance of the Kannan–Lipton Orbit Problem.

In the second case, for fixed n, one can observe that the matrix M^n is itself a matrix of rational functions. Hence the restrictions $M^n(x)u(x) = v(x)$ can be rewritten as the equations $P_i(x)/Q_i(x) = 1$ for polynomials P_i, Q_i for $i = 1, \ldots, d$. For each equation the polynomial $P_i - Q_i$ is either identically zero, or vanishes at finitely many s, which can be determined. Hence it is easy to check if there is an s in the intersection of the zero sets as i varies. This implies the following lemma, which clearly extends to a bounded region $[b, B]$ by asking for each integer $n \in [b, B]$:

Lemma IV.1. *Given n it is decidable if there exists a parameter s such that $M(s)^n u(s) = v(s)$.*

Remark. Observe that either there is some n for which $M(x)^n u(x) = v(x)$ holds for all x, 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 polynomials $P_i - Q_i$.

It remains to reduce to the two cases presented above. Our reductions to these two cases will depend on the single-parameter setting of Theorem I.1, these two cases are themselves decidable for any number of parameters. Our approach will be to place the problem into Jordan normal form (Section IV-A), where we will observe that the problem can be handled immediately if the resulting form is not diagonal (Section IV-C). In the diagonal case the problem can be reformulated for algebraic functions $\lambda_i(x), \gamma_i(x)$ for $1 \leq i \leq t$, whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that

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

We will show decidability for this in two main cases: $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle = 1$ and $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle \geq 2$ (recall Definition II.2). As discussed in the introduction, the most intriguing part of our development will be in the case of $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle \geq 2$, captured in the following lemma, which will be the major focus of our paper.

Lemma IV.2 (Main Lemma)**.** *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$ at least one of which is not constant 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*

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

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

Lemma IV.3. *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$. We assume $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle = 1$ and 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*

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

In the remainder of this section we will show how to place it into Jordan normal form and reformulate the problem in the form of these two lemmas, considering the cases where the Jordan form is not diagonal and managing the requirement in Lemma IV.2 that not all the functions are constant.

A. The parametric Jordan normal form

Let $\mathbb{K}$ be a field and $M \in \mathbb{K}^{d \times d}$ a matrix whose characteristic polynomial splits into linear factors over $\mathbb{K}$. It is well-known that we can factor M over $\mathbb{K}$ as $M = C^{-1}JC$ for some invertible matrix C and block diagonal Jordan matrix $J = \langle J_1, \ldots, J_N \rangle$, with each block J_i having the following *Jordan block* form:

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

If J_i is a $k \times k$ Jordan block associated with some eigenvalue λ, then

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

Given a matrix $M \in \mathbb{Q}(s)^{d \times d}$, recall from Section II-B that there is a connected open such subset $U \subseteq \mathbb{C}$, with $\mathbb{R} \setminus \{c_1, \ldots, c_m\} \subseteq U$, such that the characteristic polynomial of M splits into linear factors over the field $\mathbb{K}$ of algebraic functions meromorphic on U. Over the field $\mathbb{K}$ we thus have the factorisation $M = C^{-1}JC$ with J in Jordan form. The eigenvalues of M, denoted λ_1, …, λ_k, appear in the diagonal of J.

Let $\mathcal{E}$ be the finite set of point $\{c_1, \ldots, c_m\}$, the poles of the the entries of C, C^{-1} and J, and the zeros of the determinant of C (points where C is not invertible). For every $x \in \mathbb{R} \setminus \mathcal{E}$ we have $M(x) = C(x)J(x)(C(x))^{-1}$ and hence, for every $n \in \mathbb{N}$, $M^n(x)u(x) = v(x)$ if and only if $J^n(x)C^{-1}(x)u(x) = C^{-1}(x)v(x)$. On the other hand, deciding whether there exists $x \in \mathcal{E}$ with $M^n(x)u(x) = v(x)$ reduces to finitely many instances of the Kannan-Lipton Orbit Problem, which can be decided separately. We have thus reduced the parametrised point-to-point reachability problem to the following one in case of a single parameter:

Problem IV.4. *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. Define $M(x) = \begin{pmatrix} x+\frac{1}{2} & 0 & 0 \\ \frac{1}{2}-x & 1-x & 0 \\ 0 & x & 1 \end{pmatrix}$ for $x \in \mathbb{R}$. Over $\mathbb{K}$ we may write $M = C^{-1}JC$, where $J(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-x & 0 \\ 0 & 0 & x+\frac{1}{2} \end{pmatrix}$, $C(x) = \begin{pmatrix} \frac{1}{2x} & 1 & 1 \\ \frac{1}{1-4x} & 0 & 0 \\ \frac{1-2x}{4x-1} & -1 & 0 \end{pmatrix}$, and $C^{-1}(x) = \begin{pmatrix} 0 & 0 & \frac{1}{2x}-2 \\ 0 & -1 & 1-\frac{1}{2x} \\ 1 & 1 & 1 \end{pmatrix}$. 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). For $x \in \mathbb{R} \setminus \{0, 1/4\}$, all three are defined and we have $M(x) = C^{-1}(x)J(x)C(x)$, with $J(x)$ in Jordan normal form and $C(x)$ invertible.

Now, for $x = 1/4$, 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 in particular that $M(1/4)$ is non-diagonalisable (over $\overline{\mathbb{Q}}$), though M is (over $\mathbb{K}$).

Let $u = (u_1, u_2, u_3)$ and $v = (v_1, v_2, v_3)$. The problem of whether there exists $(n, s) \in \mathbb{N} \times \mathbb{R}$ for which $M(s)^n u = v$ is reduced to checking the problem at $s = 0$ and $s = 1/4$, and to the associated problem $J^n(x)\tilde{u}(x) = \tilde{v}(x)$, where

$\tilde{u}(x) = \begin{pmatrix} u_1(x)+u_2(x)+u_3(x) \\ \frac{2x}{1-4x}u_1(x) \\ \frac{1-2x}{4x-1}u_1(x)-u_2(x) \end{pmatrix}$, $\tilde{v}(x) = \begin{pmatrix} v_1(x)+v_2(x)+v_3(x) \\ \frac{2x}{1-4x}v_1(x) \\ \frac{1-2x}{4x-1}v_1(x)-v_2(x) \end{pmatrix}$, and $J^n(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (x+\frac{1}{2})^n & 0 \\ 0 & 0 & (1-x)^n \end{pmatrix}$.

B. Some simple cases

Let us now make some simplifying assumptions. In particular we define the functions $\gamma_1, \ldots, \gamma_t$ used in our reduction to Lemma IV.2 and Lemma IV.3.

Lemma IV.5. *To decide Problem IV.4 it suffices to assume that no λ_i are identically zero and that the only constant root of unity is 1 itself.*

If the row i corresponds to the row at the bottom of some Jordan cell then we rewrite the restriction $\lambda_i^n(x)\tilde{u}_i(x) = \tilde{v}_i(x)$ as $\lambda_i^n(x) = \gamma_i(x)$. To do this, we define $\gamma_i = \tilde{v}_i/\tilde{u}_i$, for the points where $u_i(s) \neq 0$. If $\tilde{u}_i$ is not constant zero then there are finitely many s where $\tilde{u}_i(s) = 0$, each of which can be handled explicitly. If some $\tilde{u}_i$ is the constant zero function then there are two cases. Firstly, if $\tilde{v}_i$ 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 $\tilde{v}_i$ not constant zero then there are only a finite number of s s.t. $0 = \tilde{v}_i(s)$. Each of these can be checked explicitly.

These observations imply that we may assume a row i corresponding to a bottom row of a Jordan block to have $\tilde{u}_i \neq 0$.

Suppose there is λ_i root of unity and γ_i not constant; then there are finitely many values which λ_i^n takes on, for each such value τ consider only the finite set of s such that $\gamma_i(s) = \tau$.

Suppose there is a λ_i root of unity and γ_i is constant. Then either there are no satisfying n or there is a regular sequence of satisfying n, that is $\lambda_i^{kn+t} = \gamma_i$ for every n. Hence the problem can be reduced to the problem for $(J(s)^k)^n(J^t(s)\tilde{u}(s)) = v(s)$, ensuring that the only root of unity is 1 itself.

If there exists λ_i not a root of unity and γ_i constant 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 the found n using Lemma IV.1 to determine if they are simultaneously satisfiable.

C. Jordan cells of dimension larger than 1

It turns out that the problem is decidable directly when $J(s)$ has a block of dimension greater than 1.

Proposition IV.6. *If $J(x)$ has a block of size ≥ 2 then the problem is decidable.*

Up to renaming the eigenvalues, assume there is a Jordan cell of dimension $k \geq 2$ corresponding to λ_1 and rows $1, \ldots, k$, where 1 is the bottom row.

There are three cases not covered by the previous section: λ_1 is not constant, λ_1 is constant but not a root of unity, or $\lambda_1 = 1$.

Let us first suppose there is a Jordan cell with $\lambda_1 = 1$. We consider the Jordan cells $J = \begin{pmatrix} 1 & 1 & & \\ 0 & 1 & 1 & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$ and observe that their powers of n describe a set of polynomial equations in variable n and coefficients in $\mathbb{K}$:

$$\Big\{\tilde{u}_1(x) = \tilde{v}_1(x), \quad \tilde{u}_2(x) + n\tilde{u}_1(x) = \tilde{v}_2(x), \ldots \sum_{i=1}^{k} \binom{n}{k} \tilde{u}_k(x) = \tilde{v}_k(x)\Big\}.$$

Clearly $\tilde{u}_1 = \tilde{v}_1$ identically, or else there are finitely many s such that $\tilde{u}_1(s) = \tilde{v}_1(s)$. Hence, the first equation can essentially be dropped. Using the second equation to replace n by $(\tilde{v}_2 - \tilde{u}_2)/\tilde{u}_1$ 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 allocations of x then we only need to check these allocations.

If all of the resulting functions are identically zero, then the system of equations is equivalent to the single equation $n = \theta(x)$, where $\theta(x) = \frac{\tilde{v}_2(x)-\tilde{u}_2(x)}{\tilde{u}_1(x)}$. 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 Lemma IV.1).

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 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:

Lemma IV.7. *Given algebraic functions $\theta(x), \lambda(x), \gamma(x)$in x, with λ not a root of unity then there is a bound on $n \in \mathbb{N}$ such that there exists a $s \in \overline{\mathbb{Q}}$ 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 II.3 we get $a_1, a_2, a_3, a_4 > 0$ such that

$$a_1 h(x) - a_2 \leq h(\theta(x)) = \log(n) \leq a_2 h(x) + a_3. \quad (3)$$

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 II.3 on the algebraic function $\gamma(x)$ we obtain c_3, c_4 such that

$$bn = h(\lambda^n) = h(\gamma(x)) \leq c_3 h(x) + c_4 \quad (4)$$

Combining Eq. (4) and Eq. (3) 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 II.3 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 Eq. (3):

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

Taken together we have

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

Returning to our Jordan blocks of size at least 2, we finally consider the case where λ_1 is a constant but not 1, or λ_1 is not a constant. Here we only need to use the bottom two rows from the block to obtain:

$$\lambda_1^n(x)\tilde{u}_1(x) = \tilde{v}_1(x)$$
$$\lambda_1^n(x)\tilde{u}_2(x) + n\lambda_1^{n-1}(x)\tilde{u}_1(x) = \tilde{v}_2(x),$$

We reformulate these equations, defining algebraic functions γ and θ:

$$\lambda_1^n(x) = \gamma_1(x) = \tilde{v}_1(x)/\tilde{u}_1(x)$$
$$n = \theta(x) = \lambda_1(x)(\tilde{v}_2(x)/\tilde{v}_1(x) - \tilde{u}_2(x)/\tilde{u}_1(x))$$

Any roots or poles of $\tilde{u}_1, \tilde{u}_2, \tilde{v}_1, \tilde{v}_2, \lambda_1$ can be handled manually (and we already ensured $\tilde{u}_1$ is not identically zero). Again we have an instance of Lemma IV.7 bounding n that need to be checked.

D. The Jordan matrix is diagonal

We may now assume that J is a diagonal matrix.

So assuming J is diagonal with eigenvalues $\lambda_1, \ldots, \lambda_t$ and we want to know if there exists $(n, s) \in \mathbb{N} \setminus \mathcal{E}$ such that

$$\lambda^n(s) = \gamma_i(s) \qquad \text{for all} \qquad i = 1, \ldots, t \tag{5}$$

Finally we make some simplifications in Lemma IV.8, in particular, not all λ_i's are constant functions when $\mathrm{rank}\langle\lambda_1, \ldots, \lambda_k\rangle \geq 2$, after which, we can invoke Lemmas IV.2 and IV.3.

Lemma IV.8. *To decide Problem IV.4, it suffices to assume that the eigenvalues 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 that either $\mathrm{rank}\langle\lambda_1, \ldots, \lambda_k\rangle = 1$ or not all λ_i's are constant.*

Proof. Consider first the case that $\lambda_1 = \lambda_2$. If $\lambda_1(x)^n = \gamma_1(x)$ and $\lambda_2(x)^n = \gamma_2(x)$, then $\gamma_1(x) = \gamma_2(x)$ either holds identically, in which case one of the equations may be removed, or holds for finitely many allocations to x, in which case the problem becomes decidable. Hence we assume that the λ_i are distinct.

We have already established, in Lemma IV.5, 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 $1^n = \gamma_j(x)$, which holds either at finitely many x or γ_j is the constant 1 and the constraint can be dropped.

Assume all λ_i's are constant functions.

If for all i we also have γ_i are constant functions then the problem is a single instance of the Kannan-Lipton Orbit Problem. In the remaining cases there is at least one γ_i non constant.

If there exists i with λ_i not a root of unity and γ_i constant 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 the found n using Lemma IV.1 to determine if they are simultaneously satisfiable.

It remains to deal with the cases where all λ_i are not roots of unity, each γ_i is not constant, and $\mathrm{rank}\{\lambda_1, \ldots, \lambda_t\} \geq 2$.

Since $\mathrm{rank} \geq 2$, we have at least two constraints and so there is λ_1 and λ_2 constant, not roots of unity, and multiplicatively independent, and γ_1, γ_2 not constant. Let the minimal polynomials of γ_i and γ_j be P_1 and P_2 with $P_i \in \overline{\mathbb{Q}}[x, y_i]$. Considering the polynomials in $\overline{\mathbb{Q}}[x, y_1, y_2]$, they have no common factors. 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 $\alpha_2 = \gamma_2(s_0)$ we have $P(\alpha_1, \alpha_2) = 0$. The sequence $(u_n)_{n=0}^{\infty}$, with

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

$a_{k,\ell} \in \overline{\mathbb{Q}}$, 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., [35]), 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 [36], 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. 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 Lemma A.5 (in Section A). $\square$

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

$$\lambda_i^{a_i}(s)^n = \gamma_i^{a_i}(s) \qquad \text{for all} \qquad (i = 1, \ldots, t). \tag{6}$$

It is clear that the set E of solutions (n, s) to (5) is a subset of the set E' of solutions to (6). 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 (6), and the problem becomes decidable. In case $\gamma_1^{a_1} = \gamma_2^{a_2} \cdots \gamma_t^{a_t}$, the first equation in (6) is redundant, and we may remove it. By repeating the process we obtain a system of the form (6) 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 (5) from the solutions to (6). 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 Lemma IV.1 finitely many times. In case both the above sets are unbounded, we give additional arguments.

V. Proof of Main Lemma (The case of $\mathrm{rank}\langle \lambda_1, \ldots, \lambda_t \rangle \geq 2$)

This part is dedicated to the proof of Lemma IV.2. By Lemma IV.8 we may assume that none of λ_i's are identically zero or a root of unity. We also 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 at the end of the previous section; here we show that there are only finitely many solutions to the reduced system, so we need not worry about creating too many new solutions.

Lemma V.1. *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 II.3 that we have

$$a_1 h(s) - a_2 \leq h(\gamma(s)) \leq a_3 h(s) + a_4$$
$$b_1 h(s) - b_2 \leq h(\lambda(s)) \leq b_3 h(s) + b_4$$

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

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

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. □

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

Proof. 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

$$c^n = \gamma_1^{a_1} \cdots \gamma_t^{a_t}(s). \tag{7}$$

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 V.2 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 II.3. Consequently, taking heights on both sides of (7), we see that $nh(c) \leq \sum_i a_i h(\gamma_i(s)) < tC'$. It is evident that n is bounded above by a constant, and the claim follows. □

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 V.3. *Assume that λ_1, λ_2, γ_1, γ_2 are 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 powerful results of Bombieri–Masser–Zannier, from which the claim is immediate.

Assume that λ_1, λ_2, γ_1, γ_2 have minimal polynomials $P_1 \in \mathbb{Q}[x, x_1]$, $P_2 \in \mathbb{Q}[x, x_2]$, $P_3 \in \mathbb{Q}[x, y_1]$, $P_4 \in P[x, y_2]$. By eliminating x from P_1 and P_i, we get polynomials $Q_1 \in \mathbb{Q}[x_1, x_2]$, $Q_2 \in P[x_1, y_1]$ and $Q_3[x_1, y_1]$, $i = 3, 4$. Let C be the curve defined by $C := \{(x_1, x_2, y_1, y_2)\colon Q_1(x_1, x_2) = Q_2(x_1, y_1) = Q_3(x_1, y_2) = 0\}$ and consider any of its finitely many absolutely irreducible components C'. We are now interested in the multiplicative relations $x_1^n = y_1$, $x_2^n = y_2$, $n \in \mathbb{N}$, along the curve C'. Notice that for any fixed n, these relations are independent in $\overline{\mathbb{Q}}^4$, i.e., one is not a consequence of the other, as they involve distinct sets of coordinates.

Let us first assume that λ_1, λ_2, γ_1, γ_2 are multiplicatively independent modulo constants. Then the set $C' \cap \overline{\mathbb{Q}}^4$ is not

contained in any set $H_{c,\vec{a}}$, $c \in \overline{\mathbb{Q}}$, $\vec{a} = (a_1, a_2, a_3, a_4) \in \mathbb{Z}^4 \setminus \{\vec{0}\}$, of the form

$$H_{c,\vec{a}} = \{(x_1, x_2, y_1, y_2) \subseteq \overline{\mathbb{Q}}^4 \colon x_1^{a_1} x_2^{a_2} y_1^{a_3} y_2^{a_4} = c\}.$$

Furthermore, notice now that the relations $x_1^n = y_1$ and $x_2^n = y_2$ are independent, that is, neither is a consequence of the other. Define further $\mathcal{H}_{1,\vec{a},\vec{b}} := \mathcal{H}_{1,\vec{a}} \cap \mathcal{H}_{1,\vec{b}}$. As an immediate consequence of [3, Thm. 2] (compare to formulation of [3, Thm.1']), the number of points in the intersection of C' and $\mathcal{H}$, where

$$\mathcal{H} := \bigcup_{n \in \mathbb{N}} H_{1,\vec{a},\vec{b}},$$

with $\vec{a}$ and $\vec{b}$ ranging over all $\mathbb{Z}$-linearly independent pairs of integer vectors, is finite. (Indeed, the sets in the union above are proper subgroups of the multiplicative group $\mathbb{G}_m^4$ of dimension 2, in the terminology of [3].) Clearly the union contains the sets $\mathcal{H}_{1,(n,0,1,0),(0,n,0,1)}$. Furthermore, by inspecting the proof of the theorem, the heights and degrees of such intersection points are effectively bounded above by a constant depending on the curve C'. This means that there are only finitely many s for which $\lambda_1(s)^n = \gamma_2(s)$ and $\lambda_2(s)^n = \gamma_2(s)$, and such s can be effectively computed. The problem is thus decidable, and we are done for the case that λ_1, λ_2, γ_1, γ_2 are multiplicatively independent modulo constants.

Assume then that λ_1, λ_2, γ_1, γ_2 are multiplicatively dependent modulo constants but are multiplicatively independent. Then curve C' is contained in some $\mathcal{H}_{c,\vec{a}}$ with c not a root of unity (again, the functions would be multiplicatively dependent were c a root of unity). The dimension of this set is at most 3, so by [4, Thm.], the set of points intersecting C and $\mathcal{H}$ defined above is finite, and the bounds of the degrees and heights for such points are effective to compute by inspecting the proof. We may thus conclude as in the above case. □

To complete with the proof of Lemma IV.2, we need to show the claim holds when λ_1, λ_2, γ_1, γ_2 are multiplicatively dependent, while λ_1 and λ_2 are multiplicatively independent modulo constants. We shall follow the reasoning made in the previous lemma, with minor modifications. 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

$$\begin{aligned} \lambda_1(s)^{nc} &= \gamma_1(s)^c \\ \lambda_2(s)^{na} &= \gamma_2(s)^a = \lambda_1(s)^{a_1} \lambda_2(s)^{a_2} \gamma_1(s)^{a_3}. \end{aligned}$$

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

Consider the family of vectors $\vec{a}_n = (nc, 0, -c)$ and $\vec{b}_n = (-a_1, na - a_2, -a3)$. Clearly, if the vectors are collinear, then $n = a/a_2$. So, save for this particular n, the sets $\mathcal{H}_{1,\vec{a}_n,\vec{b}_n}$ are of dimension at most 2, and are therefore subsets of $\mathcal{H}$ as defined above. We may handle the case of $n = a_2/a$ an integer by Lemma IV.1 separately. Assume for now that λ_1, λ_2, γ_1 are multiplicatively independent. Consider the curve C defined by these functions (similar to the construction in the above lemma), and let 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 above lemma utilising, [3, Thm. 2] for all the admissible n.

If the functions are multiplicatively dependent modulo constants, we may apply theorem [4, Thm.]. (This is essentially a theorem of Liardet [37] made effective in [38]. See also second remark after Thm. 2 in [3] and discussion following the statement of Conj. A of [4].)

So 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

$$\begin{aligned} \lambda_1(s)^{ncb} &= \gamma_1(s)^{cb} = \lambda_1(s)^{b_1 c} \lambda_2(s)^{b_2 c} \\ \lambda_2(s)^{nab} &= \lambda_1(s)^{ba_1} \lambda_2(s)^{ba_2} \gamma_1(s)^{ba_3} \\ &= \lambda_1(s)^{ba_1 + a_3 b_1} \lambda_2(s)^{a_2 b + b_2 a_3}. \end{aligned}$$

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

$$\begin{aligned} 1 &= \lambda_1(s)^{ncb - b_1 c} \lambda_2(s)^{-b_2 c} \\ 1 &= \lambda_1(s)^{-ba_1 - a_3 b_1} \lambda_2(s)^{nab - a_2 b}. \end{aligned}$$

Notice that now neither cb nor ab equals 0 according to our choices. Let now $\vec{a}_n = (ncb - b_1 c, -b_2 c)$ and $\vec{b}_n = (-ba_1 - a_3 b_1, nab - a_2 b)$. It is evident that for n larger than a computable bound, the vectors $\vec{a}_n$ and $\vec{b}_n$ are not $\mathbb{Z}$-linearly dependent. We may again solve the problem for n less than this bound using Lemma IV.1.

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 [3, Thm. 2] to conclude as above.

We have exhausted all the possibilities, so the proof of Main Lemma is complete.

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

In this section we recall and prove the following lemma:

Lemma IV.3. *Let $\lambda_1, \ldots, \lambda_t$ be algebraic functions in $\mathbb{K}$. We assume $\operatorname{rank}\langle \lambda_1, \ldots, \lambda_t \rangle = 1$ and 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*

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

We prove Lemma IV.3 by first showing that without loss of generality there is a single equation $\lambda^n(s) = \gamma$. We then separate into the case where λ is real over $\mathbb{R}$ (Section VI-B) and the case where λ is complex (Section VI-C).

A. W.l.o.g. there is a single equation

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. We get $\lambda^{b+a} = |\lambda|^b$, and taking absolute values both sides, we get $|\lambda|^a = 1$, which implies that $|\lambda| = 1$ 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 IV.8. 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.

B. Only real eigenvalues

We assume there is a single function for which we ask $\lambda^n(s) = \gamma(s)$, with λ not a constant function in s.

Lemma VI.1. *Given a 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 $\lambda^n(s) = \gamma(s)$.*

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 $0 \leq |\lambda| < 1$, or $|\lambda| > 1$, with the finite set of points $\{s : \lambda(s) = 1\}$ excluded and handled separately (recall, by Lemma IV.5 and Lemma IV.8 λ is not constant 0 or 1). We will focus on the subsets where $|\lambda| \leq 1$. Given such a subset S_i, we only need to consider each interval $D \subseteq S_i$ where $\{s \mid 0 \leq |\gamma(s)| \leq 1\}$. 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 $b = \sup_x \gamma_i(x)$

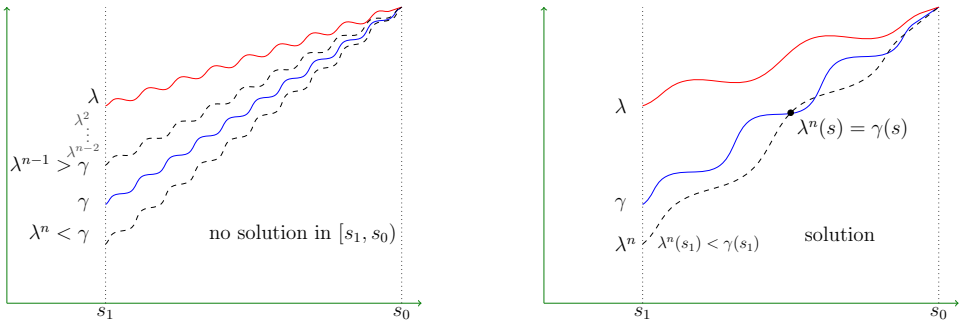

Fig. 1. Cases for $\lambda(s) \to 1$ as $s \to s_0$.

and decide whether there exists n such that $a \leq \lambda_i^n \leq b$. 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 $n \geq 0$. 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 VI.2. *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 $n \geq n_{\delta,\delta'}$ 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 $n \leq n_{\delta,\delta'}$ can be found by Lemma IV.1.

Recall, we can assume, without loss of generality we assume λ, γ are positive, if necessary by taking even or odd subsequences. 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 VI.3. *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 VI.4. *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[3], 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 VI.3, 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 VI.4, 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, Lemma IV.1). 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 Lemma IV.1).

C. With complex eigenvalues

We consider a single equation $\lambda(s)^n = \gamma(s)$, for $n \in \mathbb{N}$ and s in some open interval. Both functions have constant modulus 1. We show the following:

Lemma VI.5. *For all large enough n, the equation admits a solution.*

[3]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 $\lambda'(x)$

Assume first that λ is a constant and of modulus 1 and not a root of unity. If γ is not of constant modulus 1, then there are only finitely many s for which γ intersects the unit circle. The problem then becomes decidable as multiple instances of the Kannan–Lipton Orbit Problem. 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_1 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.

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: $\lambda = \exp(\mathrm{i}\theta(x))$, $\gamma = \exp(\mathrm{i}\psi(x))$, 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. 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 the interval be s_0 and s_1. Assume $\psi(s_0) > \theta(s_0)$ (if not, add 2π to $\psi(s_0)$). We have $\theta(s_0) < \psi(s_0)$. Now $\theta(s_1) \geq \psi(s_0) + 4\pi + \psi(s_0) \geq \psi(s_0) + 2\pi > \psi(s_1)$. Consequently, by the intermediate value theorem, there must be a point where the values $n\theta$ and ψ coincide, as they are continuous functions.

VII. Conclusion

We consider a parametric variant of the orbit problem for linear dynamical systems. Our paper shows hardness for four parameters or more, by using the parameters to describe the hyperplane of the Skolem problem. On the other hand, we show decidability with one parameter. The decidability status for two and three parameters are natural candidates for future work; there is no immediate hardness since Skolem-like problems are decidable for low dimensional targets [5], but on the other hand our number-theoretic analysis does not immediately extend to multi-parameter algebraic functions.

References

[1] R. Kannan and R. J. Lipton, "Polynomial-time algorithm for the orbit problem," *J. ACM*, vol. 33, no. 4, pp. 808–821, 1986. [Online]. Available: https://doi.org/10.1145/6490.6496

[2] M. A. Harrison, *Lectures on Linear Sequential Machines*. USA: Academic Press, Inc., 1969.

[3] E. Bombieri, D. Masser, and U. Zannier, "Intersecting a curve with algebraic subgroups of multiplicative groups," *International Mathematics Research Notices*, vol. 1999, no. 20, pp. 1119–1140, 1999.

[4] ——, "Intersecting curves and algebraic subgroups: conjectures and more results," *Transactions of the American Mathematical Society*, vol. 358, no. 5, pp. 2247–2257, 2006.

[5] V. Chonev, J. Ouaknine, and J. Worrell, "The orbit problem in higher dimensions," in *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, ser. STOC '13, New York, NY, USA, 2013. doi: 10.1145/2488608.2488728 p. 941–950.

[6] ——, "The polyhedron-hitting problem," in *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, ser. SODA '15. USA: Society for Industrial and Applied Mathematics, 2015, p. 940–956.

[7] S. Almagor, J. Ouaknine, and J. Worrell, "The Polytope-Collision Problem," in *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, ser. LIPIcs, I. Chatzigiannakis, P. Indyk, F. Kuhn, and A. Muscholl, Eds., vol. 80, Dagstuhl, Germany, 2017. doi: 10.4230/LIPIcs.ICALP.2017.24 pp. 24:1–24:14.

[8] C. Baier, F. Funke, S. Jantsch, T. Karimov, E. Lefaucheux, J. Ouaknine, A. Pouly, D. Purser, and M. A. Whiteland, "Reachability in Dynamical Systems with Rounding," in *40th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2020)*, ser. LIPIcs, N. Saxena and S. Simon, Eds., vol. 182, Dagstuhl, Germany, 2020. doi: 10.4230/LIPIcs.FSTTCS.2020.36 pp. 36:1–36:17.

[9] B. Jonsson and K. G. Larsen, "Specification and refinement of probabilistic processes," in *Proceedings Sixth Annual IEEE Symposium on Logic in Computer Science*, 1991, pp. 266–277.

[10] R. Givan, S. Leach, and T. Dean, "Bounded-parameter Markov decision processes," *Artificial Intelligence*, vol. 122, no. 1, pp. 71 – 109, 2000. doi: 10.1016/S0004-3702(00)00047-3

[11] I. Kozine and L. Utkin, "Interval-valued finite Markov chains," *Reliable Computing*, vol. 8, pp. 97–113, 04 2002. doi: 10.1023/A:1014745904458

[12] S. Junges, E. Abraham, C. Hensel, N. Jansen, J.-P. Katoen, T. Quatmann, and M. Volk, "Parameter synthesis for Markov models," 2019.

[13] R. Lanotte, A. Maggiolo-Schettini, and A. Troina, "Parametric probabilistic transition systems for system design and analysis," *Formal Asp. Comput.*, vol. 19, pp. 93–109, 03 2007. doi: https://doi.org/10.1007/s00165-006-0015-2

[14] M. Češka, F. Dannenberg, M. Kwiatkowska, and N. Paoletti, "Precise parameter synthesis for stochastic biochemical systems," in *Computational Methods in Systems Biology*, P. Mendes, J. O. Dada, and K. Smallbone, Eds. Cham: Springer International Publishing, 2014, pp. 86–98.

[15] M. Cubuktepe, N. Jansen, S. Junges, J.-P. Katoen, and U. Topcu, "Synthesis in pMDPs: A tale of 1001 parameters," in *Automated Technology for Verification and Analysis*, S. K. Lahiri and C. Wang, Eds. Cham: Springer International Publishing, 2018, pp. 160–176.

[16] E. Bartocci, R. Grosu, P. Katsaros, C. R. Ramakrishnan, and S. A. Smolka, "Model repair for probabilistic systems," in *Tools and Algorithms for the Construction and Analysis of Systems*, P. A. Abdulla and K. R. M. Leino, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 326–340.

[17] S. Pathak, E. Ábrahám, N. Jansen, A. Tacchella, and J.-P. Katoen, "A greedy approach for the efficient repair of stochastic models," in *NASA Formal Methods*, K. Havelund, G. Holzmann, and R. Joshi, Eds. Cham: Springer International Publishing, 2015, pp. 295–309.

[18] Y. Kwon and G. Agha, "Linear inequality LTL (iLTL): A model checker for discrete time Markov chains," in *Formal Methods and Software Engineering*, J. Davies, W. Schulte, and M. Barnett, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 194–208.

[19] V. A. Korthikanti, M. Viswanathan, G. Agha, and Y. Kwon, "Reasoning about MDPs as transformers of probability distributions," in *2010 Seventh International Conference on the Quantitative Evaluation of Systems*, 2010. doi: 10.1109/QEST.2010.35 pp. 199–208.

[20] R. Chadha, V. A. Korthikanti, M. Viswanathan, G. Agha, and Y. Kwon, "Model checking MDPs with a unique compact invariant set of distributions," in *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, 2011. doi: 10.1109/QEST.2011.22 pp. 121–130.

[21] M. Mignotte, T. Shorey, and R. Tijdeman, "The distance between terms of an algebraic recurrence sequence." *Journal für die reine und angewandte Mathematik*, vol. 1984, no. 349, pp. 63 – 76, 01 May. 1984. doi: 10.1515/crll.1984.349.63

[22] N. Vereshchagin, "Occurrence of zero in a linear recursive sequence," *Mathematical notes of the Academy of Sciences of the USSR*, vol. 38, pp. 609–615, 1985.

[23] V. Chonev, J. Ouaknine, and J. Worrell, "On the Skolem Problem for Continuous Linear Dynamical Systems," in *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, ser. LIPIcs, I. Chatzigiannakis, M. Mitzenmacher, Y. Rabani, and D. Sangiorgi, Eds., vol. 55, Dagstuhl, Germany, 2016. doi: 10.4230/LIPIcs.ICALP.2016.100 pp. 100:1–100:13.

[24] S. Akshay, T. Antonopoulos, J. Ouaknine, and J. Worrell, "Reachability problems for Markov chains," *Inf. Process. Lett.*, vol. 115, no. 2, p. 155–158, Feb. 2015. doi: 10.1016/j.ipl.2014.08.013. [Online]. Available: https://doi.org/10.1016/j.ipl.2014.08.013

[25] R. Majumdar, M. Salamati, and S. Soudjani, "On Decidability of Time-Bounded Reachability in CTMDPs," in *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, ser. LIPIcs, A. Czumaj, A. Dawar, and E. Merelli, Eds., vol. 168, Dagstuhl, Germany, 2020. doi: 10.4230/LIPIcs.ICALP.2020.133. ISBN 978-3-95977-138-2. ISSN 1868-8969 pp. 133:1–133:19. [Online]. Available: https://drops.dagstuhl.de/opus/volltexte/2020/12540

[26] J. Piribauer and C. Baier, "On Skolem-Hardness and Saturation Points in Markov Decision Processes," in *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, ser. LIPIcs, A. Czumaj, A. Dawar, and E. Merelli, Eds., vol. 168, Dagstuhl, Germany, 2020. doi: 10.4230/LIPIcs.ICALP.2020.138 pp. 138:1–138:17.

[27] A. Ostafe and I. Shparlinski, "On the Skolem problem and some related questions for parametric families of linear recurrence sequences," 2020. [Online]. Available: https://arxiv.org/abs/2005.06713

[28] H. Cohen, *A Course in Computational Algebraic Number Theory*. Springer Publishing Company, Incorporated, 2010. ISBN 3642081428

[29] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Berlin, Heidelberg: Springer-Verlag, 2006. ISBN 3540330984

[30] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms - an introduction to computational algebraic geometry and commutative algebra*, 2nd ed., ser. Undergraduate texts in mathematics. Springer, 1997. ISBN 978-0-387-94680-1

[31] M. Mignotte, *Some Useful Bounds*. Vienna: Springer Vienna, 1982, pp. 259–263.

[32] H. Derksen, E. Jeandel, and P. Koiran, "Quantum automata and algebraic groups," *Journal of Symbolic Computation*, vol. 39, no. 3, pp. 357–371, 2005. doi: 10.1016/j.jsc.2004.11.008 Special issue on the occasion of MEGA 2003.

[33] P. Habegger, "Quasi-Equivalence of Heights and Runge's Theorem," in *Number Theory–Diophantine Problems, Uniform Distribution and Applications*. Springer, 2017, pp. 257–280.

[34] J. Ouaknine and J. Worrell, "On the positivity problem for simple linear recurrence sequences,," in *Automata, Languages, and Programming*, J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 318–329, extended version with proofs https://arxiv.org/abs/1309.1550.

[35] J. W. S. Cassels, *Local Fields*, ser. London Mathematical Society Student Texts. Cambridge University Press, 1986.

[36] J. Berstel and M. Mignotte, "Deux propriétés décidables des suites récurrentes linéaires," *Bulletin de la Société Mathématique de France*, vol. 104, pp. 175–184, 1976. doi: 10.24033/bsmf.1823

[37] P. Liardet, "Sur une conjecture de Serge Lang," in *Journées arithmétiques de Bordeaux*, ser. Astérisque. Société mathématique de France, 1975, no. 24–25. [Online]. Available: www.numdam.org/item/AST_1975__24-25__187_0/

[38] A. Bérczes, K. Gyory, J.-H. Evertse, and C. Pontreau, "Effective results for points on certain subvarieties of tori," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 147, no. 1, 2009, p. 69.

[39] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki, "Skolem's Problem - On the Border between Decidability and Undecidability," Tech. Rep. 683, 2005.

[40] A. Baker and G. Wüstholz, "Logarithmic forms and group varieties," *Journal für die reine und angewandte Mathematik*, vol. 1993, no. 442, pp. 19–62, 1993. doi: 10.1515/crll.1993.442.19

[41] K. Yu, "P-adic logarithmic forms and group varieties I," *Journal für die reine und angewandte Mathematik*, vol. 1998, no. 502, pp. 29 – 92, 1998. doi: 10.1515/crll.1998.090

[42] ——, "p-adic logarithmic forms and group varieties II," *Acta Arithmetica*, vol. 89, pp. 337–378, 1999. doi: 10.4064/aa-89-4-337-378

APPENDIX A
DEGENERATE CASE: ARGUMENT FOR TWO CONSTANT EIGENVALUES

In this last part we deal with the remaining case of Lemma IV.8. Recall that we assume that λ_1 and λ_2 are constants that are not roots of unity, and that γ_1 and γ_2 are not constant functions.

We recall some notions from algebraic number theory. Most of the results appear in standard text books on the topic such as [28], but an accessible account sufficient for our purposes can be found in [39]. 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 [40]:

Theorem A.1 (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 A.2. *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 [34, Cor. 8 of Extended Version].

We shall also employ a p-adic version of Baker's theorem proved by K. Yu [41]. We employ a version which follows from a version stated in the introduction of K. Yu [42] (for definitions, we refer to [28]):

Theorem A.3. *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 A.4. *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 logarithmically in n. □

We formulate a lemma which completes the proof of Lemma IV.8.

Lemma A.5. *Suppose λ_1, λ_2 are constant, not roots of unity, and are multiplicatively independent. Assume further that γ_1, γ_2 are non constant functions, and have distinct minimal polynomials. Then the system $\lambda_1^n = \gamma_1(s)$, $\lambda_2^n = \gamma_2(s)$ has only finitely many solutions.*

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

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

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

Claim A.6. *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. 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 $i, j \in \mathbb{Z}$. 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 faster than $c|\lambda_1^k \lambda_2^\ell|^n + \mathcal{O}(|\lambda_1^k \lambda_2^\ell|^{n-1})$ for some computable non-zero constant c. This bound is clearly computable. □

In case the assumption of the above lemma holds, the problem becomes decidable using Lemma IV.1 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 A.7. *If $\alpha \neq 1$, then there exists an effectively computable constant $n_0 \in \mathbb{N}$, such that if $u_n \neq 0$ 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 $H(x, y)$ vanishes at most finitely many times. 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 A.2 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 $|P(\lambda_1^n, \lambda_2^n)| = D(\alpha^d)^n/n^A + \mathcal{O}(\alpha^{d-1})$ for some non-zero constant D. Again we have an effectively computable n_0 after which no solution can occur. □

Again, we may invoke Lemma IV.1 to search among the finitely many n which witness a zero in $(u_n)_n$.

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

Claim A.8. *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 A.5 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 $\nu_{\mathfrak{p}}(\lambda_1) \neq 0$. 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 larger than some computable constant, we have 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 A.4 $\nu_{\mathfrak{p}}(\lambda_2^n - \beta_i) \leq C_i \log n$ 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.