

The Orbit Problem for Parametric Linear Dynamical Systems

Christel Baier  

Technische Universität Dresden, Germany

Simon Jantsch  

Technische Universität Dresden, Germany

Engel Lefauchaux  

Max Planck Institute for Software Systems,
Saarland Informatics Campus,
Saarbrücken, Germany

Joël Ouaknine  

Max Planck Institute for Software Systems,
Saarland Informatics Campus,
Saarbrücken, Germany

Markus A. Whiteland  

Max Planck Institute for Software Systems,
Saarland Informatics Campus,
Saarbrücken, Germany

Florian Funke  

Technische Universität Dresden, Germany

Toghrul Karimov  

Max Planck Institute for Software Systems,
Saarland Informatics Campus,
Saarbrücken, Germany

Florian Luca  

School of Mathematics, Wits University,
Johannesburg, South Africa
Research Group in Algebraic Structures & Applications,
King Abdulaziz University,
Thuwal, Saudi Arabia
Max Planck Institute for Software Systems,
Saarland Informatics Campus,
Saarbrücken, Germany

David Purser  

Max Planck Institute for Software Systems,
Saarland Informatics Campus,
Saarbrücken, Germany

James Worrell  

Department of Computer Science,
University of Oxford, UK

Abstract

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

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

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

2012 ACM Subject Classification Theory of computation \rightarrow Logic and verification

Keywords and phrases Orbit problem, parametric, linear dynamical systems

Digital Object Identifier 10.4230/LIPIcs.CONCUR.2021.28

Related Version *Full Version (with full proofs)*: <https://arxiv.org/abs/2104.10634>

Funding This work was funded by DFG grant 389792660 as part of TRR 248 – CPEC (see perspicuous-computing.science), the Cluster of Excellence EXC 2050/1 (CeTI, project ID 390696704, as part of Germany's Excellence Strategy), DFG-projects BA-1679/11-1 and BA-1679/12-1, and the Research Training Group QuantLA (GRK 1763).

Joël Ouaknine: ERC grant AVS-ISS (648701). Also affiliated with Keble College, Oxford as emmy.network Fellow.

James Worrell: Supported by EPSRC Fellowship EP/N008197/1.



© Christel Baier, Florian Funke, Simon Jantsch, Toghrul Karimov, Engel Lefauchaux, Florian Luca, Joël Ouaknine, David Purser, Markus A. Whiteland, and James Worrell;
licensed under Creative Commons License CC-BY 4.0

32nd International Conference on Concurrency Theory (CONCUR 2021).

Editors: Serge Haddad and Daniele Varacca; Article No. 28; pp. 28:1–28:17



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

The *Orbit Problem* for linear dynamical systems asks to decide, given a square matrix $M \in \mathbb{Q}^{d \times d}$ and two vectors $u, v \in \mathbb{Q}^d$, whether there exists a natural number n such that $M^n u = v$. The problem was shown decidable (in polynomial time) by Kannan and Lipton [26] over ten years after Harrison first raised the question of decidability [23]. The current paper is concerned with a generalisation of the Orbit Problem to *parametric* linear dynamical systems. In general, parametric models address a major drawback in quantitative verification, namely the unrealistic assumption that quantitative data in models are known *a priori* and can be specified exactly. In applications of linear dynamical systems to automated verification, parameters are used to model partially specified systems (e.g., a faulty component with an unknown failure rate, or when transition probabilities are only known up to some bounded precision) as well as to model the unknown environment of a system. Interval Markov chains can also be considered as a type of parametric linear dynamical system.

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

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

Thus our main decidability result is as follows:

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

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

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

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

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

A further key distinction in analysing the problem in Equation (1) involves the rank of the multiplicative group generated by the functions $\lambda_1, \dots, \lambda_t$. 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 [8, Theorem 2] and [9]) concerning the intersection of a curve in \mathbb{C}^m , with algebraic subgroups of $(\mathbb{C}^*)^m$ of dimension at most $m - 2$. To apply these results we view the problem in Equation (1) geometrically in terms of whether a curve

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

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 6 a direct elementary method to find solutions of Equation (1).

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

Related work

Reachability problems in (unparametrized) linear dynamical systems have a rich history. Answering a question by Harrison [23], Kannan and Lipton [26] 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 [14]. This was extended to polytope targets in [15], and later further generalized to polytope initial sets in [2]. Orbit problems have recently been studied in the setting of rounding functions [3]. In our analysis we will make use of a version of the point-to-point reachability problem that allows matrix entries to be algebraic numbers. In this case the eigenvalues are again algebraic, and decidability follows by exactly the same argument as the rational case (although the algorithm is no longer in PTIME), and is also a special case of the main result of [10].

If the parametric matrix M is the transition matrix of a parametric Markov chain (pMC) [24, 22, 28], 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 [25]. An important problem in this direction is to find parameter settings with prescribed properties [30, 12, 19], which has also been studied in the context of model repair [4, 37]. While all previous references use the standard path-based semantics of Markov chains, the distribution transformer semantics [29, 27, 13] studies the transition behaviour on probability distributions. It has, to the best of our knowledge, never been considered for parametric Markov chains. Our approach implicitly does this in that it performs parameter synthesis for a reachability property in the distribution transformer semantics.

The Skolem Problem asks whether a linear recurrence sequence $(u_n)_n$ has a zero term (n such that $u_n = 0$). Phrased in terms of linear dynamical systems, the Skolem Problem asks whether a d -dimensional linear dynamical system hits a $(d - 1)$ -dimensional hyperplane, and decidability in this setting is known for matrices of dimension at most four [34, 39]. A continuous version of the Skolem Problem was examined in [16]. With the longstanding intractability of the Skolem Problem in general, it has recently been used as a reference point for other decision problems [1, 32, 38].

Ostafe and Shparlinski [35] consider the Skolem Problem for parametric families of simple linear recurrences. More precisely, they consider linear recurrences of the form $u_n = a_1(x)\lambda_1(x)^n + \dots + a_k(x)\lambda_k^n(x)$ 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 outside an exceptional set of numbers of bounded height (note that any value of the parameter such that the sequence u_n has a zero is necessarily algebraic).

2 Preliminaries

We denote by $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \overline{\mathbb{Q}}$ the real, complex, rational, and algebraic numbers respectively. For a field K and a finite set X of variables, $K[X]$ and $K(X)$ respectively denote the ring of polynomials and field of rational functions with coefficients in K . A meromorphic function¹ $f: U \rightarrow \mathbb{C}$ where U is some open subset $U \subseteq \mathbb{C}^\ell$ is called algebraic, if $P(x_1, \dots, x_\ell, f(x_1, \dots, x_\ell)) = 0$ for some $P \in \mathbb{Q}[x_1, \dots, x_\ell, y]$. We say that f is *real algebraic* if it is real-valued on real inputs.

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

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

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

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

2.1 Computation with algebraic numbers

Throughout this note we employ notions from (computational) algebraic geometry and algebraic number theory. Our approach relies on transforming the matrices we consider in Jordan normal form. Doing so, the coefficients of the computed matrix are not rational anymore but algebraic. Next we recall the necessary basics and refer to [17, 40] for more background on notions utilised throughout the text.

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

The algebraic numbers $\overline{\mathbb{Q}}$ are the complex numbers which can be defined as some root of a univariate polynomial in $\mathbb{Q}[x]$. In particular, the rational numbers are algebraic numbers. For every $\alpha \in \overline{\mathbb{Q}}$ there exists a unique monic univariate polynomial $P_\alpha \in \mathbb{Q}[x]$ of minimum degree for which $P_\alpha(\alpha) = 0$. We call P_α the *minimal polynomial* of α . An algebraic number α is represented as a tuple $(P_\alpha, \alpha^*, \varepsilon)$, where $\alpha^* = a_1 + a_2i$, $a_1, a_2 \in \mathbb{Q}$, is an approximation of α , and $\varepsilon \in \mathbb{Q}$ is sufficiently small such that α is the unique root of P_α within distance ε of α^* (such ε can be computed by the root-separation bound, due to Mignotte [33]). This is referred to as the *standard* or *canonical representation* of an algebraic number. Given canonical representations of two algebraic numbers α and β , one can compute canonical representations of $\alpha + \beta$, $\alpha\beta$, and α/β , all in polynomial time.

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

For all $\alpha, \beta \in \overline{\mathbb{Q}}$ and $n \in \mathbb{Z}$ we have from [40, Chapt. 3]:

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

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

2.2 Univariate algebraic functions

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

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

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

In case $L = \mathbb{Q}$, we may take K to be an algebraic number field. In particular, the eigenvalues of a rational matrix are algebraic. However, in this paper, the entries of our matrix are *algebraic functions*, and so too are the entries in Jordan normal form. We recall some basics of algebraic geometry and univariate algebraic functions required for the analysis in the single-parameter setting, and refer the reader to [5, 18] for further information.

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

occur. Furthermore, the function $1/f$ is meromorphic (on a possibly different domain U) and satisfies $y^d P(x, 1/y) = a_d(x) + \dots + a_1(x)y^{d-1} + a_0(x)y^d$. We conclude that a pole of f (a zero of $1/f$) is a zero of $a_d(x)$.

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

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

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

for all points $x \in U$ (see, e.g., [21, Chapt. 1, Thm. 8.9]).

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

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

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

2.2.1 Multiplicative relations

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

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

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

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

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

Proof. This is essentially a special case of a result from [20]. Indeed, in Sect. 3.2, they show how to find the generators of the group L in case the λ_i are elements of a finitely generated field over \mathbb{Q} . We apply the result to the field $\mathbb{Q}(x, \lambda_1, \dots, \lambda_t)$ to obtain the claim for the set L . For L' , Case 3 of [20, Sect. 3.2] computes a generating set as an intermediate step in the computation of a basis of L . Specifically, L and L' are the respective kernels of the maps φ and $\tilde{\varphi}$ in [20, Sect. 3.2]. We give an alternative proof sketch specialised to univariate functions in the full version. \blacktriangleleft

3 The Multi-Parameter Orbit Problem is Skolem-hard

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

It suffices to only consider the instances of Skolem Problem at order 5 of the form $u_n = a\lambda_1^n + \overline{a\lambda_1^n} + b\lambda_2^n + \overline{b\lambda_2^n} + c\rho^n = 0$ with $|\lambda_1| = |\lambda_2| \geq |\rho|$ and $a, b, \lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$, $c, \rho \in \mathbb{Q} \cap \mathbb{R}$, as the instances of the Skolem Problem at order 5 that are not of this form are known to be decidable [36]. We may assume that $c = \rho = 1$ by considering the sequence $(u_n/c\rho^n)$ if necessary. We can also rewrite $u_n = A\operatorname{Re}\lambda_1^n + B\operatorname{Im}\lambda_1^n + C\operatorname{Re}\lambda_2^n + D\operatorname{Im}\lambda_2^n + 1$ for $A, B, C, D \in \overline{\mathbb{Q}} \cap \mathbb{R}$.

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

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

To compute Z , first observe that $\operatorname{Im}\lambda_2^n = \pm \sqrt{(\operatorname{Re}\lambda_1^n)^2 + (\operatorname{Im}\lambda_1^n)^2 - (\operatorname{Re}\lambda_2^n)^2}$ for all n as $|\lambda_1| = |\lambda_2|$. Motivated by this observation, let $S_+, S_- \subseteq \mathbb{R}^3$, $S_+ = \{(x, y, z) : Ax + By + Cz + D\sqrt{x^2 + y^2 - z^2} + 1 = 0\}$ and $S_- = \{(x, y, z) : Ax + By + Cz - D\sqrt{x^2 + y^2 - z^2} + 1 = 0\}$. We will choose $Z = \{(x, y, z, \sqrt{x^2 + y^2 - z^2}) : (x, y, z) \in S_+\} \cup \{(x, y, z, -\sqrt{x^2 + y^2 - z^2}) : (x, y, z) \in S_-\}$. It is easy to check that the above definition of Z satisfies the requirement that $u_n = 0$ if and only if $(\operatorname{Re}\lambda_1^n, \operatorname{Im}\lambda_1^n, \operatorname{Re}\lambda_2^n, \operatorname{Im}\lambda_2^n) \in Z$, and it remains to show that both S_+ and S_- can be parametrized using algebraic functions in two variables and two parameters. To this end, observe that S_+ and S_- are both semi-algebraic subsets of \mathbb{R}^3 , but are also contained in the algebraic set $S = \{(x, y, z) : (Ax + By + Cz + 1)^2 = D^2(x^2 + y^2 - z^2)\} \subseteq \mathbb{R}^3$. Since $S \neq \mathbb{R}^3$ (for example, $(0, 0, 0) \notin S$), and it is algebraic, S can have *dimension* (see [18] for a definition) at most 2. Hence S_+, S_- also have semi-algebraic dimension at most 2. In the full version, we show that a semi-algebraic subsets of \mathbb{R}^3 of dimension at most two can be written as a finite union of sets of the form $\{v(s, t) : s, t \in \mathbb{R}\}$, where v is an algebraic function. This completes the construction of Z and the description of the reduction.

4 Single Parameter Reachability: Overview of proof

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

In our case analysis, we often show that either there is a finite set of parameter values for which the constraints could hold, or place an upper bound on the n for which the constraints hold. The following proposition shows that the decidability of the problem in these cases is apparent:

► **Proposition 8.**

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

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

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

As a consequence, for each n either $M^n u = v$ holds identically (for every s), or there are at most finitely many s such that $M(s)^n u(s) = v(s)$, and all such points are algebraic, as they must be the roots of the algebraic functions P_i .

Our approach will be to place the problem into Jordan normal form (Section 4.1), where we will observe that the problem can be handled if the resulting form is not diagonal (Section 4.2). Here the relation between the Weil height of an algebraic number and its image under an algebraic function are exploited to bound n (reducing to the second case of the preceding proposition).

In the diagonal case the problem can be reformulated for algebraic functions λ_i, γ_i for $i = 1 \dots, t$, whether there exist $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda_i^n(s) = \gamma_i(s)$ for all $i = 1, \dots, t$, where \mathcal{E} is a finite set of exceptional points. These exceptional points can be handled separately using the first case of the preceding proposition.

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

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

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

The proof of this lemma is shown in Section 5. Here we apply two specialised arguments, in the case of non-constant λ 's we exploit the results of Bombieri, Masser, and Zannier [8, 9] to show there is a finite effective set of parameter values. In the case of constant λ 's we reduce to an instance of Skolem's problem that we show is decidable, effectively bounding n .

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

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

The proof of this lemma (in Section 6), reduces the problem to a single equation ($t = 1$), for which we provide a specialised analysis on the behaviour of such functions that enable us to decide the existence of a solution.

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

4.1 The parametric Jordan normal form

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

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

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

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

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

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

28:10 The Orbit Problem for Parametric Linear Dynamical Systems

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

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

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

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

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

4.2 Jordan cells of dimension larger than 1

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

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

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

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

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

We reformulate these equations, defining algebraic function θ :

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

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

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

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

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

4.3 Further simplifying assumptions for diagonal matrices

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

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

Finally we make some simplifications in Lemma 16:

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

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

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

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

4.4 Multiplicative dependencies

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

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

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

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

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

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

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

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

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

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

5.1 All λ_i 's constant

In this section we sketch the proof for the case where λ_i 's are all constant. We reduce to a special case of the Skolem problem, but show that this particular instance is decidable. Since $\text{rank} \geq 2$, we have at least two constraints and so there are constants λ_1 and λ_2 , not roots of unity, and multiplicatively independent, with γ_1, γ_2 not constant.

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

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

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

$a_{k, \ell} \in \overline{\mathbb{Q}}$, is a linear recurrence sequence over $\overline{\mathbb{Q}}$, and we wish to characterise those n for which $u_n = 0$. By the famous Skolem–Mahler–Lech theorem (see, e.g., [11]), the set of such n is the union of a finite set and finitely many arithmetic progressions. Furthermore, it is decidable whether such a sequence admits infinitely many elements, and all the arithmetic progressions can be effectively constructed [7]. But, in general, the elements of the finite set are not known to be effectively enumerable – solving the Skolem problem for arbitrary LRS essentially reduces to checking whether this finite set is empty. However, the case at hand can be handled using now standard techniques involving powerful results from transcendental number theory, such as Baker's theorem for linear forms in logarithms, and similar results on linear forms in p -adic logarithms (see, e.g., [34, 39]). We show there exists an effectively computable $n_0 \in \mathbb{N}$ such that $u_n \neq 0$ for all $n \geq n_0$. We give a brief sketch (a detailed proof appears in the full version):

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

If the values $|\lambda_1|$ and $|\lambda_2|$ are multiplicatively dependent but neither is of modulus 1, we may again use an asymptotic argument. For this, we need Baker's theorem on linear forms in logarithms to show that a (related) sequence grows in modulus as $c\alpha^n/n^D + o(\beta^n)$, with $\beta < \alpha$ and effectively computable constants c, D . On the other hand, if $|\lambda_i| = 1$ but λ_i is an algebraic integer (a root of a monic polynomial with coefficients in \mathbb{Z}), then it will have a

Galois conjugate (roots of the minimal polynomial of λ_1) $\tilde{\lambda}_1$ with $|\tilde{\lambda}_1| > 1$. Hence a suitable Galois conjugate of the sequence (u_n) will be of the form considered in the previous case, and the zeros of (u_n) and (\tilde{u}_n) coincide. The asymptotic argument can be applied to (\tilde{u}_n) .

The final case is when λ_1 and λ_2 are not algebraic integers. We turn to the theory of prime-ideal decompositions of the numbers λ and argue, employing a version of Baker's theorem for p -adic valuations (as in [39]) to conclude similarly that the n for which $u_n = 0$ are effectively bounded above. ◀

5.2 At least one non-constant

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

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

► **Theorem 18** ([8, Theorem 2]). *Let \mathcal{C} be an absolutely irreducible (irreducible in $\overline{\mathbb{Q}}(x)$) curve defined over $\overline{\mathbb{Q}}$ in \mathbb{C}^d . Assume that the coordinates of the curve are multiplicatively independent modulo constants (i.e., the points $(x_1, \dots, x_d) \in \mathcal{C}(\overline{\mathbb{Q}})$ do not satisfy $x_1^{a_1} \cdots x_d^{a_d} = c$ identically for any $(a_1, \dots, a_d) \in \mathbb{Z}^d \setminus \vec{0}$, $c \in \overline{\mathbb{Q}}$). Then the points $(x_1, \dots, x_d) \in \mathcal{C}(\overline{\mathbb{Q}})$ for which x_1, \dots, x_d satisfy at least two independent multiplicative relations form a finite set.*

We note that given the curve \mathcal{C} , the finite set of points (x_1, \dots, x_d) on \mathcal{C} for which x_1, \dots, x_d satisfy at least two independent multiplicative relations can be effectively constructed. Indeed, this is explicitly mentioned in the last paragraph of the introduction of [8]: the proof goes by showing effective bounds on the degree and height of such points.

Theorem 18 holds for curves in \mathbb{C}^d for arbitrary d . If one allows the coordinates on the curve to satisfy a non-trivial multiplicative relation, then there can be infinitely many such points [8]. On the other hand, in [9] Bombieri, Masser, and Zannier consider relaxing the assumption of multiplicative independence modulo constants to multiplicative independence and conjecture that the conclusion of the above theorem still holds [9, Conj. A]. Supporting the conjecture, [9] proves a theorem which will suffice for us.

► **Theorem 19.** *Let \mathcal{C} be an absolutely irreducible curve in \mathbb{C}^d defined over $\overline{\mathbb{Q}}$. Assume that the coordinates of the curve are multiplicatively independent, but \mathcal{C} is contained in a set of the form $\vec{b}H$, where H is the set of points in $\overline{\mathbb{Q}}^d$ satisfying at least $d - 3$ independent multiplicative relations². Then the points $(x_1, \dots, x_d) \in \mathcal{C}(\overline{\mathbb{Q}})$ for which x_1, \dots, x_d satisfy at least two independent multiplicative relations form a finite set.*

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

Let us proceed case by case.

² With $b = (b_1, \dots, b_k)$, here $\vec{b}H = \{(b_1x_1, \dots, b_kx_k) : (x_1, \dots, x_k) \in H\}$ is a coset of a subgroup of dimension at most 3 in the terminology of [9].

³ In [8, 9] the proof is given for $d \geq 4$, and is constructive, while the case of $d = 3$ is attributed to a (non-constructive) result of Liardet [31]. A completely effective proof of the case can be found in [6].

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

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

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

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

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

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

Otherwise $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ are multiplicatively dependent modulo constants but are multiplicatively independent. Then \mathcal{C}' is contained in a set of the form $\vec{b}H$, where H satisfies at least one multiplicative relation. Applying Theorem 19 with $d = 4$, the points on \mathcal{C}' satisfying $x_1^n = x_3$ and $x_2^n = x_4$ for any $n \geq 1$, form an effectively constructible finite set. ◀

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

► **Lemma 22.** *Assume that $\lambda_1, \lambda_2, \gamma_1, \gamma_2$ are multiplicatively dependent, while λ_1, λ_2 are multiplicatively independent modulo constants. Then there exists a computable constant n_0 such that system (2) admits no solutions for $n > n_0$.*

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

This section recalls and sketches the proof of Lemma 10.

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

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

► **Lemma 23.** *Suppose $\text{rank}\langle\lambda_1, \dots, \lambda_t\rangle = 1$, then whether there is a solution $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ to $\lambda_i^n(s) = \gamma_i(s)$ for all $i = 1, \dots, t$ reduces to instances with $t = 1$.*

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

► **Lemma 24.** *Given real algebraic functions λ and γ , it is decidable whether there exists $(n, s) \in \mathbb{N} \times \mathbb{R} \setminus \mathcal{E}$ such that $\lambda^n(s) = \gamma(s)$.*

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

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

► **Lemma 25.** *Let λ and γ be algebraic functions. Assume λ is not real, non-zero, not a root of unity, and of modulus 1. The equation $\lambda(s)^n = \gamma(s)$ admits solutions as follows. If γ is not of modulus 1 constantly, then there are finitely many s . If γ is of modulus 1 identically and λ is constant, then there are infinitely many solutions and such a solution can be effectively found. Finally, if λ is not constant, then the equation admits a solution for all $n \geq n_0$, and n_0 is computable.*

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

References

- 1 S. Akshay, Timos Antonopoulos, Joël Ouaknine, and James Worrell. Reachability problems for Markov chains. *Inf. Process. Lett.*, 115(2):155–158, 2015. doi:10.1016/j.ipl.2014.08.013.
- 2 Shaul Almagor, Joël Ouaknine, and James Worrell. The Polytope-Collision Problem. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, volume 80 of *LIPICs*, pages 24:1–24:14, Dagstuhl, Germany, 2017. doi:10.4230/LIPICs.ICALP.2017.24.
- 3 Christel Baier, Florian Funke, Simon Jantsch, Toghrol Karimov, Engel Lefauchaux, Joël Ouaknine, Amaury Pouly, David Purser, and Markus A. Whiteland. Reachability in Dynamical Systems with Rounding. In Nitin Saxena and Sunil Simon, editors, *40th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2020)*, volume 182 of *LIPICs*, pages 36:1–36:17, Dagstuhl, Germany, 2020. doi:10.4230/LIPICs.FSTTCS.2020.36.
- 4 Ezio Bartocci, Radu Grosu, Panagiotis Katsaros, C. R. Ramakrishnan, and Scott A. Smolka. Model repair for probabilistic systems. In Parosh Aziz Abdulla and K. Rustan M. Leino, editors, *Tools and Algorithms for the Construction and Analysis of Systems*, pages 326–340, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.
- 5 Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Springer-Verlag, Berlin, Heidelberg, 2006.

- 6 Attila Bérczes, Kálmán Gyory, Jan-Hendrik Evertse, and Corentin Pontreau. Effective results for points on certain subvarieties of tori. *Mathematical Proceedings of the Cambridge Philosophical Society*, 147(1):69, 2009.
- 7 Jean Berstel and Maurice Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France*, 104:175–184, 1976. doi:10.24033/bsmf.1823.
- 8 Enrico Bombieri, David Masser, and Umberto Zannier. Intersecting a curve with algebraic subgroups of multiplicative groups. *International Mathematics Research Notices*, 1999(20):1119–1140, January 1999. doi:10.1155/S1073792899000628.
- 9 Enrico Bombieri, David Masser, and Umberto Zannier. Intersecting curves and algebraic subgroups: conjectures and more results. *Transactions of the American Mathematical Society*, 358(5):2247–2257, 2006. doi:10.1090/S0002-9947-05-03810-9.
- 10 Jin-Yi Cai, Richard J Lipton, and Yechezkel Zalcstein. The complexity of the ABC problem. *SIAM Journal on Computing*, 29(6):1878–1888, 2000.
- 11 John W. S. Cassels. *Local Fields*. London Mathematical Society Student Texts. Cambridge University Press, 1986. doi:10.1017/CB09781139171885.
- 12 Milan Češka, Frits Dannenberg, Marta Kwiatkowska, and Nicola Paoletti. Precise parameter synthesis for stochastic biochemical systems. In Pedro Mendes, Joseph O. Dada, and Kieran Smallbone, editors, *Computational Methods in Systems Biology*, pages 86–98, Cham, 2014. Springer International Publishing.
- 13 Rohit Chadha, Vijay Anand Korthikanti, Mahesh Viswanathan, Gul Agha, and YoungMin Kwon. Model checking MDPs with a unique compact invariant set of distributions. In *Eighth International Conference on Quantitative Evaluation of Systems, QEST 2011, Aachen, Germany, 5-8 September, 2011*, pages 121–130. IEEE Computer Society, 2011. doi:10.1109/QEST.2011.22.
- 14 Ventsislav Chonev, Joël Ouaknine, and James Worrell. The orbit problem in higher dimensions. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, STOC '13*, page 941–950, New York, NY, USA, 2013. doi:10.1145/2488608.2488728.
- 15 Ventsislav Chonev, Joël Ouaknine, and James Worrell. The polyhedron-hitting problem. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '15*, page 940–956, USA, 2015. Society for Industrial and Applied Mathematics.
- 16 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the Skolem Problem for Continuous Linear Dynamical Systems. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, volume 55 of *LIPICs*, pages 100:1–100:13, Dagstuhl, Germany, 2016. doi:10.4230/LIPICs.ICALP.2016.100.
- 17 Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer Publishing Company, Incorporated, 2010.
- 18 David A. Cox, John Little, and Donal O’Shea. *Ideals, varieties, and algorithms - an introduction to computational algebraic geometry and commutative algebra*. Undergraduate texts in mathematics. Springer, 2 edition, 1997.
- 19 Murat Cubuktepe, Nils Jansen, Sebastian Junges, Joost-Pieter Katoen, and Ufuk Topcu. Synthesis in pMDPs: A tale of 1001 parameters. In Shuvendu K. Lahiri and Chao Wang, editors, *Automated Technology for Verification and Analysis*, pages 160–176, Cham, 2018. Springer International Publishing.
- 20 Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. *Journal of Symbolic Computation*, 39(3):357–371, 2005. Special issue on the occasion of MEGA 2003. doi:10.1016/j.jsc.2004.11.008.
- 21 Otto Foster. *Compact Riemann Surfaces*, volume 81 of *Graduate Textbooks in Mathematics*. Springer, 1981. doi:10.1007/978-1-4612-5961-9.
- 22 Robert Givan, Sonia Leach, and Thomas Dean. Bounded-parameter Markov decision processes. *Artificial Intelligence*, 122(1):71–109, 2000. doi:10.1016/S0004-3702(00)00047-3.
- 23 Michael A. Harrison. *Lectures on Linear Sequential Machines*. Academic Press, Inc., USA, 1969.

- 24 Bengt Jonsson and Kim Guldstrand Larsen. Specification and refinement of probabilistic processes. In *Proceedings of the Sixth Annual Symposium on Logic in Computer Science (LICS '91), Amsterdam, The Netherlands, July 15-18, 1991*, pages 266–277. IEEE Computer Society, 1991. doi:10.1109/LICS.1991.151651.
- 25 Sebastian Junges, Erika Abraham, Christian Hensel, Nils Jansen, Joost-Pieter Katoen, Tim Quatmann, and Matthias Volk. Parameter synthesis for Markov models, 2019.
- 26 Ravindran Kannan and Richard J. Lipton. Polynomial-time algorithm for the orbit problem. *J. ACM*, 33(4):808–821, 1986. doi:10.1145/6490.6496.
- 27 Vijay Anand Korthikanti, Mahesh Viswanathan, Gul Agha, and YoungMin Kwon. Reasoning about MDPs as transformers of probability distributions. In *QEST 2010, Seventh International Conference on the Quantitative Evaluation of Systems, Williamsburg, Virginia, USA, 15-18 September 2010*, pages 199–208. IEEE Computer Society, 2010. doi:10.1109/QEST.2010.35.
- 28 Igor Kozine and Lev Utkin. Interval-valued finite Markov chains. *Reliable Computing*, 8:97–113, April 2002. doi:10.1023/A:1014745904458.
- 29 YoungMin Kwon and Gul Agha. Linear inequality LTL (iLTL): A model checker for discrete time Markov chains. In Jim Davies, Wolfram Schulte, and Mike Barnett, editors, *Formal Methods and Software Engineering*, pages 194–208, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.
- 30 Ruggero Lanotte, Andrea Maggiolo-Schettini, and Angelo Troina. Parametric probabilistic transition systems for system design and analysis. *Formal Asp. Comput.*, 19:93–109, March 2007. doi:10.1007/s00165-006-0015-2.
- 31 Pierre Liardet. Sur une conjecture de Serge Lang. In *Journées arithmétiques de Bordeaux*, number 24–25 in Astérisque. Société mathématique de France, 1975. URL: www.numdam.org/item/AST_1975__24-25__187_0/.
- 32 Rupak Majumdar, Mahmoud Salamati, and Sadegh Soudjani. On Decidability of Time-Bounded Reachability in CTMDPs. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *LIPICs*, pages 133:1–133:19, Dagstuhl, Germany, 2020. doi:10.4230/LIPICs.ICALP.2020.133.
- 33 Maurice Mignotte. *Some Useful Bounds*, pages 259–263. Springer Vienna, Vienna, 1982. doi:10.1007/978-3-7091-3406-1_16.
- 34 Maurice Mignotte, Tarlok N. Shorey, and Robert Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik*, 1984(349):63–76, 01 May. 1984. doi:10.1515/crll.1984.349.63.
- 35 Alina Ostafe and Igor Shparlinski. On the Skolem problem and some related questions for parametric families of linear recurrence sequences, 2020.
- 36 Joël Ouaknine and James Worrell. Decision problems for linear recurrence sequences. In Alain Finkel, Jérôme Leroux, and Igor Potapov, editors, *Reachability Problems*, pages 21–28, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. doi:10.1007/978-3-642-33512-9_3.
- 37 Shashank Pathak, Erika Ábrahám, Nils Jansen, Armando Tacchella, and Joost-Pieter Katoen. A greedy approach for the efficient repair of stochastic models. In Klaus Havelund, Gerard Holzmann, and Rajeev Joshi, editors, *NASA Formal Methods*, pages 295–309, Cham, 2015. Springer International Publishing.
- 38 Jakob Piribauer and Christel Baier. On Skolem-Hardness and Saturation Points in Markov Decision Processes. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *LIPICs*, pages 138:1–138:17, Dagstuhl, Germany, 2020. doi:10.4230/LIPICs.ICALP.2020.138.
- 39 Nikolay K. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical notes of the Academy of Sciences of the USSR*, 38:609–615, 1985.
- 40 Michel Waldschmidt. *Heights of Algebraic Numbers*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000. doi:10.1007/978-3-662-11569-5_3.