On the Subspace Orbit Problem and the Simultaneous Skolem Problem

Piotr Bacik
University of Oxford, UK
Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany

Anton Varonka
TU Wien, Austria

Abstract

The Orbit Problem asks whether the orbit of a point under a matrix reaches a given target set. When the target is a single point, the problem was shown to be decidable in polynomial time by Kannan and Lipton. This decidability result was later extended by Chonev et al. to targets of dimension 3 (in arbitrary ambient dimension), but decidability remains open for subspaces of dimension 4. At the other extreme, the special case of the Orbit Problem in which the target set is a hyperplane of co-dimension 1 is equivalent to the Skolem Problem for linear recurrence sequences, whose decidability has been open for many decades.

In this paper, we show that the Orbit Problem is decidable if the target subspace has dimension logarithmic in the dimension of the orbit. Over the rationals, we moreover obtain a complexity bound $\mathbf{NP}^{\mathbf{RP}}$ in this case, when the target space dimension is bounded. On the other hand, we show that the version of the Orbit Problem where the dimension of the target subspace is linear in the dimension of the orbit is as hard as the Skolem Problem.

2012 ACM Subject Classification Theory of computation → Design and analysis of algorithms; Theory of computation → Logic and verification; Computing methodologies → Algebraic algorithms

Keywords and phrases Orbit Problem, Skolem Problem, Simultaneous Skolem Problem, Linear Recurrence Sequences, Verification

Digital Object Identifier 10.4230/LIPIcs.LICS.2026.8

Related Version *Extended Version*: `https://arxiv.org/abs/2601.18349` [8]

Funding *Piotr Bacik*: Supported by EPSRC grant EP/X033813/1, ERC grant DynAMiCs 101167561 and DFG grant 389792660 as part of TRR 248.
Anton Varonka: Supported by the ERC consolidator grant ARTIST 101002685.
This paper is part of a project that has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 10103444).

Acknowledgements The authors would like to thank Joël Ouaknine and James Worrell for helpful comments. The authors would like to express gratitude to the organisers of the SAMSA 2025 workshop, who provided a fertile ground for the ideas that led to this paper.

1 Introduction

A *linear dynamical system* (LDS) consists of a matrix $A \in \mathbb{K}^{d\times d}$ and initial vector $\boldsymbol{x} \in \mathbb{K}^d$, where $\mathbb{K}$ is a field. An LDS $(A, \boldsymbol{x})$ defines an *orbit* $\mathcal{B}(A, \boldsymbol{x}) = \{\boldsymbol{x}, A\boldsymbol{x}, A^2\boldsymbol{x}, \dots\}$ given by the image of $\boldsymbol{x}$ under repeated application of A. The Orbit Problem, introduced by Harrison [18] in the context of the reachability problem for linear sequential machines, asks whether a given LDS $(A, \boldsymbol{x}) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ reaches a given point $\boldsymbol{y} \in \mathbb{Q}^d$, that is, whether $\boldsymbol{y} \in \mathcal{B}(A, \boldsymbol{x})$. A decade later, this problem was shown to be decidable in polynomial time by Kannan and Lipton [20, 19].

A natural generalisation to the problem where the target point $\boldsymbol{y}$ is replaced by a target subspace $S \subseteq \mathbb{Q}^d$ was discussed in the journal version of their work [19].

> **Subspace Orbit Problem.**
> Given an LDS $(A, \boldsymbol{x}) \in \mathbb{K}^{d\times d} \times \mathbb{K}^d$ and a subspace $S \subseteq \mathbb{K}^d$, decide whether $\mathcal{B}(A, \boldsymbol{x}) \cap S \neq \varnothing$.

Around 30 years later, a significant step forward was achieved by Chonev, Ouaknine and Worrell [13, 14], who showed the Subspace Orbit Problem is in $\mathbf{NP}^{\mathbf{RP}}$ when the dimension of the target subspace is at most 3, regardless of the dimension d of the ambient space. To date, this is the state of the art for the Subspace Orbit Problem, with decidability for higher-dimensional target subspaces remaining a major open problem.

Other domains for targets have been studied in [15, 4, 25], among which one finds polyhedra and more generally semi-algebraic sets. Cumulatively, we call these problems the *orbit problems*. A plethora of further generalisations and variants of orbit problems may be found in the literature [9, 3, 24, 16, 17]. An important application of the orbit problems comes from program analysis: note that LDS can be viewed as linear while loops

$$\boldsymbol{v} \leftarrow \boldsymbol{x};\ \ \textbf{while}\ \textsc{cond}(v)\ \textbf{do}\ \ \boldsymbol{v} \leftarrow A \cdot \boldsymbol{v},$$

where reachability of a target S corresponds to the halting problem with $\textsc{cond}(\boldsymbol{v}) = \boldsymbol{v} \notin S$; that is, where the looping condition is expressed as a finite disjunction of linear disequalities. We refer the reader to [22, 33, 23] for further discussions of LDS and loops.

Taking one step back, a major obstruction on the way to deciding orbit problems is the Skolem Problem. A *linear recurrence relation* of order d over a field $\mathbb{K}$ is an equation

$$u_n = c_1 u_{n-1} + \cdots + c_d u_{n-d}, \tag{1.1}$$

where $c_i \in \mathbb{K}$ for $1 \leq i \leq d$ and $c_d \neq 0$. A linear recurrence sequence (LRS) $u = \langle u_n \rangle_{n\in\mathbb{N}}$ is a sequence of elements in $\mathbb{K}$ satisfying (1.1). In the case that $\mathbb{K}$ has characteristic 0, the set $\mathcal{Z}(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zero terms of an LRS is described by the theorem of Skolem, Mahler, and Lech [35, 29, 27]:

▶ **Theorem 1** (Skolem–Mahler–Lech). *The zero set $\mathcal{Z}(u)$ is a union of finitely many arithmetic progressions and a finite set.*

The proof is unfortunately ineffective – though we can find the arithmetic progressions, there is no known algorithm to compute the exceptional finite set. Computing this finite set is equivalent to solving the *Skolem Problem*.

> **Skolem Problem.**
> Given an LRS u, decide whether $\mathcal{Z}(u)$ is non-empty.

We denote the Skolem Problem on $\mathbb{K}$-LRS that satisfy a recurrence relation of order d as $\textsc{Skolem}_{\mathbb{K}}(d)$; when $\mathbb{K} = \overline{\mathbb{Q}}$ we simply write $\textsc{Skolem}(d)$. It is straightforward to see that deciding the Skolem Problem is equivalent to deciding the Subspace Orbit Problem with a hyperplane target, that is, a linear subspace of $\mathbb{K}^d$ of dimension $d-1$. However, despite being posed close to a century ago, decidability of the Skolem Problem has stubbornly remained open; decidability is known for $\textsc{Skolem}(4)$ [36, 38, 5], and furthermore, $\textsc{Skolem}_{\mathbb{Q}}(4)$ lies in **coRP** [7], but $\textsc{Skolem}_{\mathbb{Q}}(5)$ remains open [11]. In the orbit problems terminology, the decidability of reaching a 4-dimensional subspace of $\mathbb{Q}^5$ is open.

When considering *non-degenerate* sequences, the statement of Theorem 1 can be further refined. Define the *characteristic polynomial* of u satisfying Equation (1.1) to be

$$g(x) = x^d - c_1 x^{d-1} - \cdots - c_d \,.$$

We say u is non-degenerate if no ratio of distinct roots of its characteristic polynomial is a root of unity. The Skolem–Mahler–Lech Theorem shows that a non-degenerate LRS is either identically zero or has finitely many zero terms. Crucially, for every LRS $\langle u_n \rangle_{n\in\mathbb{N}}$ there exists an integer L such that each subsequence $\langle u_{Ln+r} \rangle_{n\in\mathbb{N}}$ with $0 \le r \le L-1$ is non-degenerate.

The Reduced Subspace Orbit Problem

The Subspace Orbit Problem with target space $S \subseteq \mathbb{Q}^5$ of dimension 4 is equivalent to $\textsc{Skolem}_{\mathbb{Q}}(5)$, the decidability of which appears to be beyond the reach of current methods. A natural question is to ask whether the problem with target dimension 4 becomes tractable when the dimension of the LDS is sufficiently large. However, for this we need a sufficiently robust notion of the dimension of an LDS. For example, if $(A, \boldsymbol{x}) \in \mathbb{K}^{d\times d} \times \mathbb{K}^d$, then one might naïvely take the dimension of $(A, \boldsymbol{x})$ to be the ambient dimension d. We argue against it, as any LDS may trivially be viewed as being inside a space of arbitrarily large dimension by adding new components to $A, \boldsymbol{x}$ that are zero everywhere. Instead, we introduce the notion of *reduced* LDS, and of the *inherent* dimension of an LDS.

Call a LDS $(A, \boldsymbol{x})$ *non-degenerate* if no ratio of distinct eigenvalues of the matrix A is a root of unity. Define the *Krylov dimension* of an orbit to be the smallest dimension of any subspace that contains it. We say an LDS $(A, \boldsymbol{x}) \in \overline{\mathbb{Q}}^{d\times d} \times \overline{\mathbb{Q}}^d$ is *reduced* if it is non-degenerate and the Krylov dimension of any tail of its orbit is d; that is, $\dim \operatorname{span}\{A^n \boldsymbol{x} : n \ge m\} = d$ for all $m \ge 0$.

By removing finitely many initial points, taking sub-orbits and restricting to smaller subspaces (see Section 2), the orbit of any LDS may be rewritten as a union of finitely many points, and finitely many orbits of reduced LDS with equal Krylov dimensions. We define the *inherent dimension* of an LDS to be the Krylov dimension of its associated reduced LDS.[1] The inherent dimension may be more intuitively characterised by the following property: if an LDS has inherent dimension d then its orbit cannot be contained within a finite union of dimension $d-1$ subspaces.

It turns out that the notion of inherent dimension is the right one for investigating the problem at higher dimensions – although deciding the Subspace Orbit Problem for LDS of inherent dimension d and target subspaces of dimension t is $\textsc{Skolem}(5)$-hard when $(d, t) = (5, 4)$, the problem becomes tractable already when $(d, t) = (6, 4)$. This motivates the following question, which this paper investigates: **for each fixed target dimension, what is the smallest inherent dimension of LDS for which we can decide the Subspace Orbit Problem?**

The Subspace Orbit Problem on arbitrary LDS can be solved by solving the Subspace Orbit Problem on each associated reduced LDS. Therefore, in the rest of the paper we assume that **any LDS $(A, \boldsymbol{x})$ is reduced**, unless stated otherwise. We denote the Subspace Orbit Problem restricted to reduced LDS $(A, \boldsymbol{x}) \in \mathbb{K}^{d\times d} \times \mathbb{K}^d$ and subspaces $S \subseteq \mathbb{K}^d$ of dimension t by $\textsc{Orbit}_{\mathbb{K}}(d, t)$.

[1] Reduced LDS have the property that their Krylov dimension remains the same upon removing finitely many points or taking sub-orbits, so the notion of inherent dimension is well defined.

We investigate the central question via the Simultaneous Skolem Problem, also discussed in [6].

Simultaneous Skolem Problem.
Given a finite set of LRS $u^{(1)}, \ldots, u^{(k)}$, decide whether

$$\mathcal{Z}(u^{(1)}, \ldots, u^{(k)}) = \{n \in \mathbb{N} : u_n^{(i)} = 0 \text{ for all } 1 \le i \le k\}$$

is non-empty.

Moreover, we are interested in computing the set $\mathcal{Z}(u^{(1)}, \ldots, u^{(k)})$. While the Skolem Problem corresponds to the Subspace Orbit Problem where targets are hyperplanes, the Simultaneous Skolem Problem can express any subspace target.

We further denote the Simultaneous Skolem Problem on k linearly independent[2] non-degenerate $\mathbb{K}$-LRS satisfying the same recurrence relation of order d by $\textsc{SimSkolem}_{\mathbb{K}}(d, k)$.

Just like how the Subspace Orbit Problem for general LDS reduces to considering reduced LDS, the Simultaneous Skolem Problem for general LRS reduces to linearly independent and non-degenerate LRS by passing to non-degenerate subsequences and removing linearly dependent LRS. We shall see that while known algorithms only yield $\mathcal{Z}(u)$ for u of order at most 4, considering $k \ge 2$ LRS simultaneously renders decidable problems for LRS of higher orders.

Overview of the results

When $\mathbb{K} = \overline{\mathbb{Q}}$, we omit the subscript, i.e. $\textsc{Orbit}_{\overline{\mathbb{Q}}}(d, t) = \textsc{Orbit}(d, t)$ and $\textsc{SimSkolem}_{\overline{\mathbb{Q}}}(d, k) = \textsc{SimSkolem}(d, k)$.

We first show that deciding $\textsc{Orbit}(d, t)$ is equivalent to deciding $\textsc{SimSkolem}(d, d-t)$.[3] We then study $\textsc{SimSkolem}(d, k)$, in which the key observation is that all simultaneous zeros of $u^{(1)}, \ldots, u^{(k)}$ are zeros of an arbitrary linear combination $w = \sum_{i=1}^{k} \alpha_i u^{(i)}$ of these LRS. $\textsc{SimSkolem}$ may thus be solved by solving the Skolem Problem for $\langle w_n \rangle_{n \in \mathbb{N}}$. More precisely, provided that $u^{(1)}, \ldots, u^{(k)}$ are non-degenerate and linearly independent, any non-trivial linear combination w of these LRS is a non-zero non-degenerate LRS. By Theorem 1, the zero set $\mathcal{Z}(w)$ is finite; if we can compute it exactly, all that is left to do in order to compute $\mathcal{Z}(u^{(1)}, \ldots, u^{(k)})$ is to check whether $u_n^{(i)} = 0$ for each $n \in \mathcal{Z}(w)$ and all $1 \le i \le k$. The freedom to choose the linear combination w plays a crucial role in achieving our decidability results. Using this, we show decidability of

- $\textsc{SimSkolem}(6, 2)$ and $\textsc{Orbit}(6, 4)$,
- $\textsc{SimSkolem}(9, 4)$ and $\textsc{Orbit}(9, 5)$,
- $\textsc{SimSkolem}(12, 6)$ and $\textsc{Orbit}(12, 6)$.

We provide examples that show that these results are the best possible with the techniques we use, even when restricting to $\textsc{SimSkolem}_{\mathbb{Q}}(d, k)$ and $\textsc{Orbit}_{\mathbb{Q}}(d, t)$.

In addition to these low-dimensional results, we show that **for each target dimension, the Subspace Orbit Problem is decidable whenever the inherent dimension of the LDS is sufficiently large.** In particular, we show the following.

---

[2] Say $u^{(1)}, \ldots, u^{(k)}$ are linearly dependent if there exist $b_1, \ldots, b_k \in \overline{\mathbb{Q}}$ such that $b_1 u_n^{(1)} + \cdots + b_k u_n^{(k)} = 0$, for all $n \in \mathbb{N}$.

[3] Note that in conjunction with the simple observation that $\textsc{SimSkolem}(d, k)$ reduces to $\textsc{SimSkolem}(d-1, k-1)$ (see Lemma 15) and the fact that $\textsc{Skolem}(4)$ is decidable [5], this already extends the decidability results of Chonev et. al. [14] from vector spaces over $\mathbb{Q}$ to vector spaces over $\overline{\mathbb{Q}}$.

▶ **Theorem 2.** $\textsc{SimSkolem}(d,k)$ *is decidable for all* (d,k) *satisfying* $d-k \leq 2\log_3 d$. *Equivalently,* $\textsc{Orbit}(d,t)$ *is decidable whenever* $t \leq 2\log_3 d$.

We provide a careful complexity analysis which shows that, for any fixed T, the problem $\textsc{Orbit}_{\mathbb{Q}}(d,t)$ for arbitrary d and $t \leq T$ satisfying $t \leq 2\log_3 d$ is in $\mathbf{NP^{RP}}$, and if d is fixed then the problem lies in **coRP**.

Finally, we provide an improved reduction of the Skolem Problem to the Subspace Orbit Problem. Specifically, we show that if there existed a constant $C \in (0,1)$ such that there was an algorithm solving $\textsc{Orbit}(d,t)$ for all $t \leq Cd$, then such an algorithm could be used to decide the Skolem Problem.

Our contributions are visually summarised in Figure 1.

	$d=1$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$	$d=7$	$d=8$	$d=9$	$d=10$	$d=11$	$d=12$	$\cdots$
$t=1$													
$t=2$			decid. by Chonev et al. (over $\mathbb{Q}$)										
$t=3$													
$t=4$					$\textsc{Skolem}(5)$	decid.	$\rightarrow$						$\cdots$
$t=5$						$\textsc{Skolem}(6)$			decid.	$\rightarrow$			$\cdots$
$t=6$							$\textsc{Skolem}(7)$	$\textsc{Skolem}_{\mathbb{Q}}(5)$				decid.	$\rightarrow$
$\vdots$								$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Figure 1 A table depicting the state of the art, and our contributions for $\textsc{Orbit}_{\overline{\mathbb{Q}}}(d,t)$.
Green: shown decidable over $\mathbb{Q}$ by [14], and extended in the present article to $\overline{\mathbb{Q}}$.
Blue: instances newly shown decidable in the present paper over $\overline{\mathbb{Q}}$; we show $\textsc{Orbit}_{\mathbb{Q}}(d,t)$ for them to be in $\mathbf{NP^{RP}}$, and in **coRP** when d is fixed.
Yellow: instances which are provably not MSTV-reducible (cf. Definition 13), as shown by Example 21.
Red: instances which are $\textsc{Skolem}_{\mathbb{Q}}(k)$-hard or $\textsc{Skolem}(k)$-hard for some k (the proof for $\textsc{Orbit}(8,6)$ is in the full version of this paper [8]).

2 Preliminaries

Reducing LDS

The *Krylov subspace* $V \subseteq \overline{\mathbb{Q}}^d$ associated to an LDS $(A, \boldsymbol{x}) \in \overline{\mathbb{Q}}^{d\times d} \times \overline{\mathbb{Q}}^d$ is the $\overline{\mathbb{Q}}$-vector space spanned by the orbit of $\boldsymbol{x}$ under the powers of $A \in \overline{\mathbb{Q}}^{d\times d}$:

$$V \coloneqq \operatorname{span}(\boldsymbol{x}, A\boldsymbol{x}, A^2\boldsymbol{x}, \dots).$$

Let $V_k \coloneqq \operatorname{span}(\boldsymbol{x}, A\boldsymbol{x}, A^2\boldsymbol{x}, \dots, A^{k-1}\boldsymbol{x})$ be a vector subspace spanned by the first k vectors of the orbit. By definition, let $V_0 \coloneqq \{\boldsymbol{0}\}$. Clearly,

$$V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k \subseteq \cdots \subseteq V. \tag{2.1}$$

Let $\mu \leq d$ be the minimum power such that $A^\mu \boldsymbol{x} \in V_\mu$. Then the increasing chain (2.1) stabilises at $k = \mu$, that is, $V_k = V_{k+1} = \cdots = V$. Moreover, μ is the dimension of the Krylov subspace V which we also call the *Krylov dimension* of V. The use of the eponym is a tribute to the seminal paper [26] by Krylov; for similar usage see e.g. [37, Part VI]. We write $\dim(A,\boldsymbol{x}) \coloneqq \mu$. If $\mu = d$ we say $(A,\boldsymbol{x})$ is *full-dimensional*. We say $(A,\boldsymbol{x})$ has *stable dimension* if $\dim(A,\boldsymbol{x}) = \dim(A, A^n\boldsymbol{x})$ for all $n \in \mathbb{N}$. Observe that $(A,\boldsymbol{x})$ certainly has stable dimension if A is invertible. The following lemma shows how we can reduce to considering invertible A, and that when taking sub-orbits, each sub-orbit has equal Krylov dimension. See also [21, Section 6.1] for similar discussion.

▶ **Lemma 3.** *Let $(A, \boldsymbol{x}) \in \overline{\mathbb{Q}}^{d\times d} \times \overline{\mathbb{Q}}^d$ be an LDS and let L be an integer. Then there exists an integer μ and an invertible matrix $M \in \overline{\mathbb{Q}}^{d\times d}$ (both depending only on A, $\boldsymbol{x}$ and L) such that for all $0 \leq r \leq L-1$, the LDS $(A^L, A^{d+r}\boldsymbol{x})$ has stable dimension μ and $\mathcal{B}(A^L, A^{d+r}\boldsymbol{x}) = \mathcal{B}(M, A^{d+r}\boldsymbol{x})$.*

Proof. First, note that if A is nilpotent then $A^n = 0$ for all $n \geq d$, and therefore the conclusion of the lemma follows trivially, with $\mu = 0$ and $M = I_d$, the $d \times d$ identity matrix. Henceforth assume A is not nilpotent, and so has some non-zero eigenvalue. Let $J = PAP^{-1}$ be the Jordan normal form with block-diagonal such that $J = \mathrm{diag}(J_1, J_2)$ with $J_1 \in \overline{\mathbb{Q}}^{d_1\times d_1}$ invertible and $J_2 \in \overline{\mathbb{Q}}^{d_2\times d_2}$ nilpotent, with $d_1 > 0$. Let $\boldsymbol{s} = P\boldsymbol{x} = (\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2)^\top$, for $\tilde{\boldsymbol{s}}_1 \in \overline{\mathbb{Q}}^{d_1}$, $\tilde{\boldsymbol{s}}_2 \in \overline{\mathbb{Q}}^{d_2}$. Then, since $J_2^n = 0$ for all $n \geq d$, we have $J^n\boldsymbol{s} = (J_1^n\tilde{\boldsymbol{s}}_1, \boldsymbol{0})^\top$ for all $n \geq d$.

Define $\tilde{J} = \mathrm{diag}(J_1, I_{d_2})$. Since $J^n\boldsymbol{s} = (J_1^n\tilde{\boldsymbol{s}}_1, \boldsymbol{0})^\top$ for all $n \geq d$, we have $J^nJ^d\boldsymbol{s} = \tilde{J}^nJ^d\boldsymbol{s}$ for all $n \geq 0$. That is, $\mathcal{B}(\tilde{J}, J^d\boldsymbol{s}) = \mathcal{B}(J, J^d\boldsymbol{s})$.

Fix an integer L. Since J_1 is invertible, $\dim(J_1^L, J_1^d\tilde{\boldsymbol{s}}_1)$ is stable; define $\mu \coloneqq \dim(J_1^L, J_1^d\tilde{\boldsymbol{s}}_1)$. For each $0 \leq r \leq L-1$, we have

$$\tilde{J}^r\mathcal{B}(\tilde{J}^L, J^d\boldsymbol{s}) = \mathcal{B}(\tilde{J}^L, J^{d+r}\boldsymbol{s}).$$

The Krylov subspaces of $(\tilde{J}^L, J^{d+r}\boldsymbol{s})$, $0 \leq r \leq L-1$, are related by multiplication by an invertible matrix. It follows that

$$\dim(\tilde{J}^L, J^d\boldsymbol{s}) = \dim(\tilde{J}^L, J^{d+1}\boldsymbol{s}) = \cdots = \dim(\tilde{J}^L, J^{d+L-1}\boldsymbol{s}) = \mu.$$

Recall that P is invertible. By letting $M = P^{-1}\tilde{J}^LP$, it follows that that $(M, A^{d+r}\boldsymbol{x})$ has stable dimension μ for each $0 \leq r \leq L-1$. Note also that M is invertible, and that $\mathcal{B}(A^L, A^{d+r}\boldsymbol{x}) = \mathcal{B}(M, A^{d+r}\boldsymbol{x})$, proving what was desired. ◀

▶ Remark 4. From the proof, we see that $\mu \leq d - d_2$, where d_2 is the multiplicity of 0 as a root of the characteristic polynomial of A.

Recall that an LDS $(A, \boldsymbol{x})$ is *reduced* if it is non-degenerate, full-dimensional and has stable dimension. Note that if $(A, \boldsymbol{x})$ is reduced then A is invertible. Indeed, if not then 0 is an eigenvalue of A and by Remark 4 we have $\mu < d$. Recall also that $\textsc{Orbit}(d, t)$ is the Subspace Orbit Problem on *reduced* LDS $(A, \boldsymbol{x}) \subseteq \overline{\mathbb{Q}}^{d\times d} \times \overline{\mathbb{Q}}^d$ and subspace $S \subseteq \overline{\mathbb{Q}}^d$ of dimension t. We now formalise a reduction from an arbitrary instance $(A, \boldsymbol{x}, S)$ of the Subspace Orbit Problem for a non-reduced LDS $(A, \boldsymbol{x}) \in \overline{\mathbb{Q}}^{d\times d} \times \overline{\mathbb{Q}}^d$ to $\textsc{Orbit}$.

First, check whether $A^i\boldsymbol{x} \in S$ for some $i < d$. If not the case, find an integer L such that A^L is non-degenerate.[4] We apply Lemma 3 to find an invertible matrix M such that $\mathcal{B}(A^L, A^{d+r}\boldsymbol{x}) = \mathcal{B}(M, A^{d+r}\boldsymbol{x})$ for all $0 \leq r \leq L-1$. Now decompose the orbit $\mathcal{B}(A, A^d\boldsymbol{x})$ into L sub-orbits $\mathcal{B}_r = \mathcal{B}(M, A^{d+r}\boldsymbol{x})$, where $0 \leq r \leq L-1$. Moreover, for each r, define $V_r \coloneqq \mathrm{span}(\mathcal{B}_r)$. These subspaces are all of dimension $\mu \leq d$ by Lemma 3, and so can be identified with $\overline{\mathbb{Q}}^\mu$. Recall that we call μ the *inherent dimension* of $(A, \boldsymbol{x})$. The new targets $S_r \coloneqq S \cap V_r$ are linear subspaces of V_r, respectively.

The original orbit $\mathcal{B}(A, \boldsymbol{x})$ reaches subspace S of dimension t if and only if at least one of the following holds: 1) $A^i\boldsymbol{x} \in S$ for some $i < d$; 2) for some r, the orbit $\mathcal{B}_r$ of the reduced LDS (in ambient dimension $\mu \leq d$) reaches the subspace $S_r \subseteq \overline{\mathbb{Q}}^\mu$ of dimension $t_r \leq t$. Now, 1) can be solved by a finite check, while 2) consists of instances of $\textsc{Orbit}(\mu, t_r)$ for each $0 \leq r \leq L-1$. We summarise this in the following statement.

[4] We may take L to be the lowest common multiple of the orders of all ratios of eigenvalues λ_i/λ_j that are roots of unity. This is at most exponential in the degree of the number field containing all eigenvalues [14, Section A.5].

▶ **Proposition 5.** *Solving the Subspace Orbit Problem on arbitrary LDS* $(A, \boldsymbol{x}) \in \overline{\mathbb{Q}}^{d\times d} \times \overline{\mathbb{Q}}^d$ *of inherent dimension* μ *and target subspace* $S \subseteq \overline{\mathbb{Q}}^d$ *of dimension* t *reduces to solving finitely many instances of* $\textsc{Orbit}(\mu, t')$ *for* $t' \leq t$*.*

Algebraic Number Theory

We recall some algebraic number theory. More details can be found in [32, 39]. Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$, i.e, a number field. We define the notions of Archimedean and non-Archimedean absolute values on $\mathbb{K}$, which are central to the decidability results we prove.

When $p \in \mathbb{Z}$ is a prime, we define the p-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by $v_p(0) = \infty$ and $v_p\left(p^r \frac{a}{b}\right) = r$, where $a, b, p \in \mathbb{Z}$ are pairwise coprime. We define the p-adic absolute value by $|x|_p = p^{-v_p(x)}$. We require a generalisation of this to number fields, via a notion of valuation with respect to a prime ideal.

Let $\mathcal{O}_\mathbb{K}$ denote the ring of algebraic integers in $\mathbb{K}$. Define a *fractional ideal* of $\mathbb{K}$ to be a non-zero finitely generated $\mathcal{O}_\mathbb{K}$-submodule of $\mathbb{K}$. Equivalently I is a fractional ideal if and only if there is $c \in \mathbb{K}$ such that $cI \subseteq \mathcal{O}_\mathbb{K}$ is an ideal of $\mathcal{O}_\mathbb{K}$. The fractional ideals of $\mathbb{K}$ form a group under multiplication. Any fractional ideal I of $\mathbb{K}$ has a unique decomposition [32, p. 22]

$$I = \prod_{i=1}^{t} \mathfrak{p}_i^{n_i} \tag{2.2}$$

where $t \in \mathbb{N}$, each $\mathfrak{p}_i \subseteq \mathcal{O}_\mathbb{K}$ is a prime ideal and $n_i \in \mathbb{Z}$.

For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_\mathbb{K}$ we define the *valuation* $v_\mathfrak{p} : \mathbb{K} \to \mathbb{Z} \cup \{\infty\}$ by $v_\mathfrak{p}(0) = \infty$ and for non-zero $a \in \mathbb{K}$, we define $v_\mathfrak{p}(a)$ to be the exponent of $\mathfrak{p}$ in the prime decomposition of the fractional ideal $a\mathcal{O}_\mathbb{K}$ given by (2.2). There is exactly one prime $p \in \mathbb{Z}$ such that $v_\mathfrak{p}(p) > 0$; we say $\mathfrak{p}$ *lies above* p, and define the ramification index $e_\mathfrak{p} = v_\mathfrak{p}(p)$. We define the $\mathfrak{p}$-adic absolute value $|x|_\mathfrak{p} = p^{-v_\mathfrak{p}(x)/e_\mathfrak{p}}$.

By Ostrowski's theorem, any (non-trivial) absolute value on $\mathbb{Q}$ is equivalent to the modulus $|\cdot|$ or a p-adic absolute value $|\cdot|_p$ for some prime $p \in \mathbb{Z}$. Furthermore, if $|\cdot|_v$ is a (non-trivial) absolute value on $\mathbb{K}$, then its restriction to $\mathbb{Q}$ is either equivalent to the modulus $|\cdot|$ (in which case $|\cdot|_v$ is *Archimedean* and we write $v \mid \infty$) or some p-adic absolute value $|\cdot|_p$ (in which case $|\cdot|_v$ is *non-Archimedean* and we write $v \mid p$, or $v \nmid \infty$). We normalise $|\cdot|_v$ such that, on $\mathbb{Q}$, $|\cdot|_v$ coincides with the modulus $|\cdot|$ or $|\cdot|_p$ for some p; in the Archimedean case we have $|x|_v = x$ for all $x \in \mathbb{Q}_{\geq 0}$ and in the non-Archimedean case $|p|_v = p^{-1}$. Denote the set of non-trivial absolute values on $\mathbb{K}$, normalised as above, by $M_\mathbb{K}$.

If $v \in M_\mathbb{K}$ is Archimedean, it either corresponds to a real embedding $\mathbb{K} \overset{\sigma}{\hookrightarrow} \mathbb{R}$ or a pair of complex embeddings $\mathbb{K} \overset{\sigma,\overline{\sigma}}{\hookrightarrow} \mathbb{C}$. In both cases, under the normalisation above we have $|x|_v = |x|_\sigma = |\sigma(x)|$. Define the *local degree* D_v of v as $D_v = 1$ or $D_v = 2$ if v corresponds to a real embedding or a pair of complex conjugate embeddings respectively.

If $v \in M_\mathbb{K}$ is non-Archimedean, and $v \mid p$, then v corresponds to a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_\mathbb{K}$ dividing p. Under the normalisation above, we have $|x|_v = |x|_\mathfrak{p} = p^{-v_\mathfrak{p}(x)/e_\mathfrak{p}}$. Define $D_v = [\mathbb{K}_v : \mathbb{Q}_p]$ where $\mathbb{K}_v, \mathbb{Q}_p$ are the completions of $\mathbb{K}, \mathbb{Q}$ with respect to $|\cdot|_v, |\cdot|_p$ respectively. Note also that any non-Archimedean $v \in M_\mathbb{K}$ satisfies the ultrametric inequality: for any $x, y \in \mathbb{K}$ we have $|x + y|_v \leq \max\{|x|_v, |y|_v\}$.

In our complexity analysis, we require a robust notion of the size of an algebraic number. This is the content of the next definition.

▶ **Definition 6.** *Define* $\log^+(x) = \log\max\{1, x\}$*. If* $x \in \mathbb{K}$ *and* $[\mathbb{K} : \mathbb{Q}] = D$*, we define the* absolute logarithmic height *of* x *(or just* height *for short) as*

$$h(x) := \frac{1}{D} \sum_{v \in M_{\mathbb{K}}} D_v \log^+ |x|_v \,.$$

It is known that the height depends only on x, not the choice of number field $\mathbb{K}$. The height satisfies the following properties, found in [39, Sections 3.2, 3.5].

▶ **Proposition 7.** *For any algebraic numbers* $\alpha_1, \alpha_2, \ldots, \alpha_m$ *with* $\alpha_1 \neq 0$*, for any* $n \in \mathbb{Z}$ *and any absolute value* $|\cdot|_v$ *on* $\mathbb{Q}(\alpha_1)$ *we have*

1. $h(\alpha_1\alpha_2) \leq h(\alpha_1) + h(\alpha_2)$,
2. $h(\alpha_1 + \cdots + \alpha_m) \leq \log m + h(\alpha_1) + \cdots + h(\alpha_m)$,
3. $h(\alpha_1^n) = |n| h(\alpha_1)$,
4. $-[\mathbb{Q}(\alpha_1) : \mathbb{Q}]h(\alpha_1) \leq \log|\alpha_1|_v \leq [\mathbb{Q}(\alpha_1) : \mathbb{Q}]h(\alpha_1)$

Linear Recurrence Sequences

Let u be a $\overline{\mathbb{Q}}$-LRS satisfying recurrence relation (1.1) of order d. Say u has order d if it does not satisfy any recurrence relation of order $d-1$. Note then Skolem(d) refers to the Skolem problem for all LRS of order $\leq d$.

A $\overline{\mathbb{Q}}$-LRS u satisfying (1.1) has an exponential polynomial form

$$u_n = \sum_{i=1}^{s} P_i(n)\lambda_i^n = \sum_{i=1}^{s}\sum_{j=0}^{m_i-1} c_{i,j} n^j \lambda_i^n \tag{2.3}$$

where each $P_i(n) = \sum_{j=0}^{m_i-1} c_{i,j} n^j \in \overline{\mathbb{Q}}[n]$ is a polynomial, and $\lambda_1, \ldots, \lambda_s$ are the roots of the *characteristic polynomial* $g(X) = X^d - c_1 X^{d-1} - \cdots - c_d$, with multiplicities $m_1, \ldots, m_s$. We call $\lambda_1, \ldots, \lambda_s$ the *characteristic roots* of u. If λ_i/λ_j is a root of unity for any $i \neq j$ then we say u is degenerate. For $|\cdot|_v$ an absolute value, call λ_i *dominant with respect to* $|\cdot|_v$ (or $|\cdot|_v$-dominant), if $|\lambda_i|_v \geq |\lambda_j|_v$ for all $j \neq i$. We say an LRS is *simple* if $\deg P_i = 0$ for all $i \in \{1, \ldots, s\}$.

We make some further definitions to discuss different parts of the LRS. Precisely, a *term* is a product of an exponential monomial $n^j\lambda_i^n$ and a non-zero constant $c_{i,j}$. If λ_i is dominant with respect to $|\cdot|_v$, then we call $c_{i,j}n^j\lambda_i^n$ a *dominant term*. Fix a linear order on the set of exponential monomials in (2.3) and associate with u a vector $\boldsymbol{u} \in \overline{\mathbb{Q}}^d$ of constants $c_{i,j}$ with respect to this order.[5] We refer to the set of non-zero components of a vector $\boldsymbol{u}$ as its *support* $\mathrm{supp}(\boldsymbol{u})$.

Given k LRS $u^{(1)}, \ldots, u^{(k)}$ satisfying (1.1), consider their associated vectors $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(k)} \in \overline{\mathbb{Q}}^d$. We say that $u^{(1)}, \ldots, u^{(k)}$ are *linearly independent* over $\overline{\mathbb{Q}}$ if the subspace $C \subseteq \overline{\mathbb{Q}}^d$ spanned by $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(k)}$ has dimension k.

3 Decidability

We formalise the connection between Orbit and SimSkolem in the following proposition.

▶ **Proposition 8.** *For any* $k \leq d$*, the problems* $\text{Orbit}_{\mathbb{K}}(d, d-k)$ *and* $\text{SimSkolem}_{\mathbb{K}}(d, k)$ *are equivalent.*

[5] Note that it is possible for the $c_{i,j}$ here to be zero, e.g. if the order of u is $< d$.

Proof. Let $(M, \boldsymbol{x}, S)$ be an instance of $\textsc{Orbit}_{\mathbb{K}}(d, d-k)$ and let $S \subseteq \mathbb{K}^d$ be a subspace spanned by $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_{d-k}\}$. Consider a basis $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_k\}$ of the orthogonal complement $S^\perp$. Then $M^n\boldsymbol{x} \in S$ iff $\boldsymbol{u}_i^\top M^n \boldsymbol{x} = 0$ for all i. Now, $\boldsymbol{u}_1^\top M^n\boldsymbol{x}, \dots, \boldsymbol{u}_k^\top M^n\boldsymbol{x}$ are all LRS that satisfy the same linear recurrence relation of order d. Indeed, let

$$g_M(X) = X^d - c_1X^{d-1} - \cdots - c_{d-1}X - c_d$$

be the characteristic polynomial of M, where $c_d \neq 0$ as M is invertible[6]. By the Cayley–Hamilton theorem, $g_M(M) = 0$, and hence, for all n and $1 \le i \le k$,

$$\boldsymbol{u}_i^\top g_M(M)M^n\boldsymbol{x} = \boldsymbol{u}_i^\top M^{n+d}\boldsymbol{x} - \cdots - c_d\boldsymbol{u}_i^\top M^n\boldsymbol{x} = 0\,.$$

The LRS are linearly independent; suppose that $\sum_{i=1}^k \alpha_i\boldsymbol{u}_i^\top M^n\boldsymbol{x} = 0$ holds for all n for some $(\alpha_1, \dots, \alpha_k) \in \mathbb{K}^k \setminus \{\boldsymbol{0}\}$. Then

$$\left(\sum_{i=1}^k \alpha_i\boldsymbol{u}_i\right)^\top M^n\boldsymbol{x} = 0$$

for all n. Since the vectors $\boldsymbol{u}_i$, $i = 1, \dots, k$, are linearly independent, we have $\sum_{i=1}^k \alpha_i\boldsymbol{u}_i \neq 0$ so the orbit $\mathcal{B}(M, \boldsymbol{x})$ is contained in a proper subspace of $\mathbb{K}^d$ which contradicts our original assumption. Finally, the characteristic roots of the LRS are exactly the eigenvalues of M, so the non-degeneracy of M implies the non-degeneracy of the LRS.

For the other direction, consider k linearly independent, non-degenerate LRS $u^{(1)}, \dots, u^{(k)}$ that satisfy the same recurrence relation

$$u_n^{(i)} = c_1u_{n-1}^{(i)} + \cdots + c_du_{n-d}^{(i)},$$

where $c_d \neq 0$. Take M to be the companion matrix of the characteristic polynomial, so $M = (\boldsymbol{e}_2 \mid \cdots \mid \boldsymbol{e}_d \mid \boldsymbol{w})$, where $\boldsymbol{w} = (c_d, \dots, c_1)^\top$. For each $i \in \{1, \dots, k\}$, let $\boldsymbol{u}_{\text{init}}^{(i)} \in \mathbb{K}^d$ denote the row vector $\boldsymbol{u}_{\text{init}}^{(i)} = \left(u_0^{(i)}, \dots, u_{d-1}^{(i)}\right)$ of initial values of the sequence $u_n^{(i)}$. These k vectors $\left\{\boldsymbol{u}_{\text{init}}^{(1)}, \dots, \boldsymbol{u}_{\text{init}}^{(k)}\right\}$ are linearly independent over $\mathbb{K}$. Now, the instance of the Simultaneous Skolem Problem is positive if and only if there exists $n \in \mathbb{N}$ such that

$$n \in \mathcal{Z}(u^{(1)}, \dots, u^{(k)}) \Leftrightarrow u_n^{(1)} = \cdots = u_n^{(k)} = 0 \Leftrightarrow$$
$$\boldsymbol{u}_{\text{init}}^{(1)}M^n\boldsymbol{e}_1 = \cdots = \boldsymbol{u}_{\text{init}}^{(k)}M^n\boldsymbol{e}_1 = 0.$$

This is equivalent to $M^n\boldsymbol{e}_1 \in S = \left\{\boldsymbol{u}_{\text{init}}^{(1)}, \dots, \boldsymbol{u}_{\text{init}}^{(k)}\right\}^\perp$ for some n, where S is a $d-k$-dimensional subspace of $\mathbb{K}^d$. Notice that $\dim(M, \boldsymbol{e}_1) = d$, since $M^{j-1}\boldsymbol{e}_1 = \boldsymbol{e}_j$ for $1 \le j \le d$, and $\boldsymbol{e}_1, \dots, \boldsymbol{e}_d$ span $\mathbb{K}^d$. Moreover, $(M, \boldsymbol{e}_1)$ has stable dimension as M is invertible, and M is non-degenerate since the $u^{(i)}$ are. Thus $(M, \boldsymbol{e}_1)$ is reduced and $(M, \boldsymbol{e}_1, S)$ forms an instance of $\textsc{Orbit}(d, d-k)$. ◀

3.1 Solving SimSkolem

▶ **Definition 9** ([5]). *The MSTV[7] class consists of algebraic LRS that have at most 3 dominant roots with respect to some Archimedean absolute value or at most 2 dominant roots with respect to some non-Archimedean absolute value.*

[6] See Remark 4 and subsequent discussion.
[7] Stands for Mignotte, Shorey, Tijdeman, and Vereshchagin.

The term was coined in [28] and named after the authors of the seminal papers [36, 38], who proved decidability of the Skolem Problem for all non-degenerate LRS in the MSTV class. In contrast to the definition in [28], the LRS we consider are over $\overline{\mathbb{Q}}$; since there are several embeddings of an arbitrary number field into $\mathbb{C}$, we have multiple Archimedean absolute values we may use, which will generally have different numbers of dominant roots, while for $\mathbb{Q}$-LRS only the modulus is used.

The idea we employ to decide SimSkolem for k LRS $u^{(1)}, \ldots, u^{(k)}$ is to take a linear combination

$$w_n = \sum_{j=1}^{k} \beta_j u_n^{(j)}$$

where we choose the $\beta_j \in \overline{\mathbb{Q}}$ to eliminate sufficiently many dominant roots and force w to fall into the MSTV class. Then all simultaneous zeros of $u^{(1)}, \ldots, u^{(k)}$ are zeros of a non-zero non-degenerate w, so the Simultaneous Skolem Problem may be solved by finding the finite zero set $\mathcal{Z}(w)$ and checking whether for some $n \in \mathcal{Z}(w)$ we have $u_n^{(i)} = 0$ for each $1 \leq i \leq k$.

Unfortunately, this method has a complication. Sometimes, the coefficients in front of the dominant roots in the exponential-polynomial representation of the LRS will be particularly pathological, and there is no way to choose a linear combination that leaves at most 3 dominant roots without eliminating all of them (at which point there are "new" dominant roots of second-largest absolute value, which complicates application of the MSTV class). Let us illustrate this vexing situation with an example.

▶ **Example 10.** Choose $\lambda_1, \ldots, \lambda_d \in \overline{\mathbb{Q}}$ such that $|\lambda_1| = \cdots = |\lambda_4| > |\lambda_5| \geq \cdots \geq |\lambda_d|$ and consider two LRS $u^{(1)}, u^{(2)}$ given by

$$u_n^{(i)} = \alpha_1^{(i)} \lambda_1^n + \alpha_2^{(i)} \lambda_2^n + \alpha_3^{(i)} \lambda_3^n + \alpha_4^{(i)} \lambda_4^n + \sum_{j=5}^{d} \alpha_j^{(i)} \lambda_j^n$$

with linearly independent vectors $(\alpha_1^{(i)}, \alpha_2^{(i)}, \alpha_3^{(i)}, \alpha_4^{(i)}, \ldots, \alpha_d^{(i)})$ for $i = 1, 2$. Suppose first that the coefficients of the $|\cdot|$-dominant roots are linearly independent, that is,

$$\left(\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_3^{(1)}, \alpha_4^{(1)}\right) \neq t \cdot \left(\alpha_1^{(2)}, \alpha_2^{(2)}, \alpha_3^{(2)}, \alpha_4^{(2)}\right)$$

for all $t \in \overline{\mathbb{Q}}$. Then it is easy to see that we can choose a linear combination $v_n = \beta_1 u_n^{(1)} + \beta_2 u_n^{(2)}$ that eliminates precisely between 1 and 3 of the dominant roots $\lambda_1, \ldots, \lambda_4$, so v is in the MSTV class. However, if the coefficients of the dominant roots are linearly dependent so that

$$\left(\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_3^{(1)}, \alpha_4^{(1)}\right) = t \cdot \left(\alpha_1^{(2)}, \alpha_2^{(2)}, \alpha_3^{(2)}, \alpha_4^{(2)}\right)$$

for some $t \in \overline{\mathbb{Q}}$, then every linear combination $v_n = \beta_1 u_n^{(1)} + \beta_2 u_n^{(2)}$ has exactly 0 or 4 of the dominant roots $\lambda_1, \ldots, \lambda_4$ remaining. In particular, if $|\lambda_5| = \cdots = |\lambda_d|$ and $d \geq 8$, it is not possible to take a linear combination that has at most 3 $|\cdot|$-dominant roots.

We note one saving grace in this situation: if the dominant terms are linearly dependent, we can eliminate more roots than expected. In particular, if $d = 8$, we can take a linear combination with at most 4 characteristic roots, which does lie in the MSTV class by the argument of [5]. This is the behaviour we shall exploit in our main results. Pathological behaviour aside, it is key to our approach to understand how many $|\cdot|_v$-dominant terms LRS may have, for each absolute value $|\cdot|_v$. This is the content of the following theorem, which is a generalisation of [5, Lemma 4.3].

▶ **Theorem 11.** *Let $\lambda_1, \dots, \lambda_r$ be $r > 1$ algebraic numbers such that no quotient λ_i/λ_j for any $i \neq j$ is a root of unity and such that*

$$|\lambda_1| = |\lambda_2| = \dots = |\lambda_r|.$$

Consider an exponential polynomial

$$f(\lambda_1, \dots, \lambda_r) = \sum_{i=1}^{r} P_i(n)\lambda_i^n = \sum_{i=1}^{r} \sum_{j=0}^{\deg P_i} c_{i,j} n^j \lambda_i^n \tag{3.1}$$

with t terms. There exists an absolute value $|\cdot|_v$ with respect to which at most $\left\lfloor \frac{t}{2} \right\rfloor$ terms of (3.1) *are dominant.*

Proof. Let $\mathbb{K}$ be a Galois number field containing $\lambda_1, \dots, \lambda_r$, with Galois group G. Consider $\mu_i = \frac{\lambda_i}{\lambda_1}$. Note that dividing each λ_i by a constant in this way does not change the number of terms that are dominant with respect to any absolute value. Moreover, $f(\lambda_1, \lambda_2, \dots, \lambda_r) = \lambda_1^n \cdot f(1, \mu_2, \dots, \mu_r)$. So it suffices to prove that there is a subset of at most $\left\lfloor \frac{t}{2} \right\rfloor$ of the terms in $f(1, \mu_2, \dots, \mu_r)$ that are dominant with respect to some absolute value. For a term $cn^k\mu^n$ we refer to the algebraic number μ as its base.

Now we have

$$1 = \mu_2\overline{\mu}_2 = \dots = \mu_r\overline{\mu}_r$$

and by applying $\sigma \in G$ to the equation we get

$$1 = \sigma(\mu_2)\sigma(\overline{\mu}_2) = \dots = \sigma(\mu_r)\sigma(\overline{\mu}_r) \tag{3.2}$$

for all $\sigma \in G$.

Case 1: $|\sigma(\mu_i)| \neq 1$ for some σ, i; either $|\sigma(\mu_i)| > 1$ or $|\sigma(\overline{\mu}_i)| > 1$.

Let $|\cdot|_\sigma$ be the absolute value defined by $|x|_\sigma = |\sigma(x)|$ and let $|\cdot|_\tau$ be the absolute value defined by $|x|_\tau = |\sigma(\overline{x})|$.[8] We argue that at most $\lfloor \frac{t}{2} \rfloor$ terms are $|\cdot|_\sigma$-dominant or at most $\lfloor \frac{t}{2} \rfloor$ terms are $|\cdot|_\tau$-dominant.

We discuss the case $|\sigma(\mu_i)| > 1$. Suppose at least $1 + \left\lfloor \frac{t}{2} \right\rfloor$ terms are dominant with respect to $|\cdot|_\sigma$, then there are at least $1 + \left\lfloor \frac{t}{2} \right\rfloor$ terms whose base μ_j satisfies $|\sigma(\mu_j)| > 1$. Therefore, by (3.2) there are at least $1 + \left\lfloor \frac{t}{2} \right\rfloor$ terms such that $|\mu_j|_\tau = |\sigma(\overline{\mu}_j)| < 1 = |1|_\tau$ for their bases μ_j. Each of these terms is non-dominant with respect to $|\cdot|_\tau$. So there are at most

$$t - \left(1 + \left\lfloor \frac{t}{2} \right\rfloor\right) \leq \left\lfloor \frac{t}{2} \right\rfloor$$

dominant terms with respect to $|\cdot|_\tau$. Note that the case where we instead assume $|\sigma(\overline{\mu}_i)| > 1$ for some i is completely symmetrical.

Case 2: $|\sigma(\mu_i)| = 1$ for all σ, i. If $v_\mathfrak{p}(\mu_2) = 0$ for all prime ideals $\mathfrak{p} \subseteq \mathcal{O}_\mathbb{K}$, then $\mu_2 \in \mathcal{O}_\mathbb{K}$; in fact, μ_2 is a unit of that ring. All Galois conjugates of μ_2 lie in the unit circle, so by Kronecker's theorem μ_2 is a root of unity. This contradicts our assumption that λ_2/λ_1 is not a root of unity. Therefore, we have $v_\mathfrak{p}(\mu_2) \neq 0$ for some prime ideal $\mathfrak{p} \subseteq \mathcal{O}_\mathbb{K}$. Then by the exact same argument as in Case 1, at most $\left\lfloor \frac{t}{2} \right\rfloor$ of the terms are dominant with respect to either $|\cdot|_\mathfrak{p}$ or the non-Archimedean absolute value $|\cdot|_v$ defined by $|x|_v = |\overline{x}|_\mathfrak{p}$. ◀

[8] The latter is an absolute value as $\tau(x) = \sigma(\overline{x})$ is a composition of Galois automorphisms so is a Galois automorphism itself.

We give an example to show that this bound is optimal – one cannot always guarantee having fewer dominant terms. In fact, this bound is optimal even when one assumes extra structure from the λ_i arising as characteristic roots of a simple *integer*-valued LRS.

▶ **Example 12.** We work with the ring of Gaussian integers $\mathbb{Z}[i]$. Recall that $\mathbb{Z}[i]$ is the ring of algebraic integers of $\mathbb{Q}(i)$ and is a PID. The Gaussian primes are exactly those of the form $a + bi$ with $a^2 + b^2$ equal to an integer prime, or $a = 0$ and $|b| \equiv 3 \bmod 4$, or $b = 0$ and $|a| \equiv 3 \bmod 4$.

We choose $s \geq 3$ Gaussian primes $p_1, \ldots, p_s \in \mathbb{Z}[i]$ such that there are no pairs of associates[9] in the set $\{p_1, \ldots, p_s, \overline{p}_1, \ldots, \overline{p}_s\}$. This can be achieved by choosing Gaussian integers of the form $a + bi$ with $|a|, |b| > 1$, as this implies $p_i, \overline{p}_i$ are not associates. Moreover, to guarantee that p_i and p_j, as well as p_i and $\overline{p}_j$, are not associates when $i \neq j$, we select $p_1, \ldots, p_s$ so that $|p_i| > |p_{i+1}|$ for all $1 \leq i \leq s - 1$.

We consider $\lambda_1, \ldots, \lambda_s \in \mathbb{Z}[i]$ given by

$$\lambda_i = \overline{p}_i \prod_{j \neq i} p_j \, .$$

Observe that $\lambda_1, \ldots, \lambda_s, \overline{\lambda}_1, \ldots, \overline{\lambda}_s$ are pairwise distinct and no two numbers in the set $\Lambda_{2s} := \{\lambda_1, \ldots, \lambda_s, \overline{\lambda}_1, \ldots, \overline{\lambda}_s\}$ are associates, as they have distinct prime factorisations.

Clearly we have $|\lambda_1| = |\overline{\lambda}_1| = \cdots = |\lambda_s| = |\overline{\lambda}_s|$. Moreover, they all have equal absolute value with respect to every Archimedean absolute value as the only other Archimedean absolute value is given by $|x|_v = |\overline{x}|$. Now, $|\cdot|_{p_i}, |\cdot|_{\overline{p}_i}$ for $i = 1, \ldots, s$ are the only non-Archimedean absolute values for which not all elements of Λ_{2s} are dominant. It is easy to see that for each i exactly s elements of Λ_{2s} are dominant in $|\cdot|_{p_i}$, and similarly for $|\cdot|_{\overline{p}_i}$.

Now, to extend our example to sets of algebraic numbers of cardinality $r = 2s + 1 \geq 7$, let

$$\lambda_{s+1} = \prod_i p_i \overline{p}_i \in \mathbb{Z} \, .$$

Then all numbers in the set $\Lambda_{2s+1} = \{\lambda_1^2, \overline{\lambda}_1^2, \ldots, \lambda_s^2, \overline{\lambda}_s^2, \lambda_{s+1}\}$ are dominant with respect to every Archimedean absolute value. For a non-Archimedean absolute value $|\cdot|_{p_i}$ (resp. $|\cdot|_{\overline{p}_i}$), exactly s of the numbers are dominant, and all are dominant with respect to every other non-Archimedean absolute value.

For every $r \geq 6$, we have constructed a set of roots Λ_r such that with respect to any absolute value at least $\lfloor \frac{r}{2} \rfloor$ of the roots are dominant. The cases $r = 4, 5$ may be handled by taking $\Lambda_4 := \{\lambda_1, \lambda_2, \overline{\lambda}_1, \overline{\lambda}_2\} \subseteq \Lambda_6$, and $\Lambda_5 := \{\lambda_1^2, \lambda_2^2, \overline{\lambda}_1^2, \overline{\lambda}_2^2, \lambda_4\} \subset \Lambda_7$. These have the desired property that all roots are dominant with respect to all Archimedean absolute values, and for each non-Archimedean absolute value there are at least 2 dominant roots.

All constructed sets Λ_r, $r \geq 4$, arise as sets of characteristic roots of simple integer-valued LRS because each $\Lambda_r \subset \mathbb{Z}[i]$ is closed under complex conjugates.

3.2 MSTV-reducibility

We now show how to use Theorem 11 to decide cases of SimSkolem (and hence of Orbit). Let $u_n^{(1)}, \ldots, u_n^{(k)}$ be non-degenerate linearly independent LRS satisfying the same recurrence relation. Recall that if we can find a linear combination w_n that lies in the MSTV class, then we can compute the zero set $\mathcal{Z}(u^{(1)}, \ldots, u^{(k)})$.

[9] Recall that $a, b \in R$ are associates if $a = bu$ for some invertible $u \in R$.

▶ **Definition 13.** *An instance* $u_n^{(1)}, \ldots, u_n^{(k)}$ *of* $\textsc{SimSkolem}(d,k)$ *is* MSTV-reducible *if there exists a non-zero linear combination* $w_n = \sum_{i=1}^{k} \beta_i u_n^{(i)}$ *with* $\beta_i \in \overline{\mathbb{Q}}$ *which lies in the MSTV class. Similarly, an instance of* $\textsc{Orbit}(d,t)$ *is MSTV-reducible if the instance of* $\textsc{SimSkolem}(d, d-t)$ *to which it reduces is MSTV-reducible.*

We refer to problems $\textsc{Orbit}(d,t)$ *and* $\textsc{SimSkolem}(d,k)$ *as MSTV-reducible (hence decidable) if all their instances are MSTV-reducible.*

Recall the representation of the LRS as vectors $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(k)}$ of coefficients; let $\pi_v, \pi_{\neg v}$ be respectively the projections onto the dominant and non-dominant components with respect to the absolute value $|\cdot|_v$. We now discuss the images of the associated subspace $C \subseteq \overline{\mathbb{Q}}^d$ under projections. Notice that an instance of $\textsc{SimSkolem}(d,k)$ is MSTV-reducible if there exists an absolute value $|\cdot|_v$ and a vector $\boldsymbol{w} \in C$ such that the projection $\pi_v(\boldsymbol{w})$ is non-zero and has support of size at most 3 (for Archimedean $|\cdot|_v$) or at most 2 (for non-Archimedean $|\cdot|_v$).[10]

The following is the lemma that guides our search for linear combinations that have few dominant terms.

▶ **Lemma 14.** *Given an instance* $\{u_n^{(i)}\}_{i=1}^{k}$ *of* $\textsc{SimSkolem}(d,k)$*, let* C *be the subspace spanned by the* k *associated vectors of these sequences. Let* ℓ *be the number of vector components that correspond to dominant terms with respect to a fixed absolute value* $|\cdot|_v$*. Then, for* $r := \dim \pi_v(C)$*,*

1. *there exist* $k-r$ *linearly independent vectors* $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{k-r} \in C$ *with* $\pi_v(\boldsymbol{w}_1) = \cdots = \pi_v(\boldsymbol{w}_{k-r}) = \boldsymbol{0}$*;*
2. *there exists* $\boldsymbol{w} \in C$ *for which* $\pi_v(\boldsymbol{w})$ *has the support of size at least 1 and at most* $\ell - r + 1$*.*

Proof. We present a constructive proof whence an algorithm computing $\boldsymbol{w}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{k-r}$ can be deduced. Let $(A \mid B)$ be the matrix whose i-th row comprises the coefficients of the sequence $u_n^{(i)}$. The columns of $A \in \overline{\mathbb{Q}}^{k\times\ell}$ correspond to the $|\cdot|_v$-dominant terms, while the columns of $B \in \overline{\mathbb{Q}}^{k\times(d-\ell)}$ are the coefficients of the remaining terms. We perform elementary row operations on $(A \mid B)$ in order to put A into row echelon form. Observe that the rows of $(A \mid B)$ are linearly independent, and so are the rows of the transformed $k \times d$ matrix at any step of this procedure. The subspace $\pi_v(C)$ is spanned by the rows of A, and hence the rank of A is r.

The rest follows from two observations. First, the row echelon form of a $k \times \ell$ matrix with rank $r > 0$ has $k - r$ zero rows. Second, the last non-zero row has at least $r-1$ zeros. ◀

▶ **Lemma 15.** *If* $\textsc{SimSkolem}(d,k)$ *is MSTV-reducible, then so is* $\textsc{SimSkolem}(d+1,k+1)$*.*

Proof. Let $\{u^{(i)}\}_{i=1}^{k+1}$ be an instance of $\textsc{SimSkolem}(d+1,k+1)$. Denote the coefficient vector of the i-th sequence by $\boldsymbol{u}^{(i)}$ and let $C := \operatorname{span}(\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(k+1)}) \subseteq \overline{\mathbb{Q}}^{d+1}$.

First, we restrict our attention to those vector components that correspond to the characteristic root λ_1. We select the non-zero component of $n^j \lambda_1^n$ with the greatest j across all $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(k+1)}$. Relabel the vector components so that the selected component is the first one. Without loss of generality, the (new) first component of $\boldsymbol{u}^{(1)}$ is non-zero. By performing one round of Gaussian elimination, it is easy to see that C contains k linearly independent vectors $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(k)}$ such that the first component of each vector is zero.

[10] Note that this actually corresponds to $\boldsymbol{w}$ having at most 3 dominant terms with respect to an Archimedean absolute value or at most 2 dominant terms with respect to a non-Archimedean absolute value, which is slightly stronger than Definition 9.

Now consider the vectors $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(k)} \in \overline{\mathbb{Q}}^d$ obtained from $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(k)}$ by eliminating the first component. By assumption there exists a linear combination $w_n = \sum_{i=1}^{k} \beta_i w_n^{(i)}$ of their associated sequences, an LRS of order at most d, which lies in the MSTV class. However, then the linear combination $v_n := \sum_{i=1}^{k} \beta_i v_n^{(i)} = w_n$ of the associated sequences of $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(k)}$ – a linear combination of the LRS $u^{(1)}, \ldots, u^{(k+1)}$ – lies in the MSTV class. ◀

The corollary below follows from applying Lemma 15 to the fact that $\textsc{SimSkolem}(4, 1) = \textsc{Skolem}(4)$ is MSTV-reducible [5].

▶ **Corollary 16.** $\textsc{SimSkolem}(d, k)$ *is MSTV-reducible for any* d, k *such that* $0 \leq d - k \leq 3$.

By Corollary 16 we moreover have that $\textsc{Orbit}(d, d-k)$ is decidable for $d - k \leq 3$ and any d. We may also interpret Lemma 15 in terms of the reduced Subspace Orbit Problem: if $\textsc{Orbit}(d, t)$ is MSTV-reducible, then $\textsc{Orbit}(d+1, t)$ is MSTV-reducible as well. From now on, our goal is to find the decidable $\textsc{SimSkolem}(d, k)$ with the least d for each fixed $d - k$.

Before moving to the decidability results for $\textsc{SimSkolem}$, we note a useful corollary of Theorem 11 which we will use repeatedly.

▶ **Corollary 17.** *For any instance of* $\textsc{SimSkolem}(d, k)$ *with characteristic roots* $\lambda_1, \ldots, \lambda_s$, *and for any* $0 < t \leq d$ *such that* $d < 2t + 2 - \left\lfloor \frac{t+1}{2} \right\rfloor$ *either there are at most* t *dominant terms with respect to some Archimedean absolute value, or there are at most* $\left\lfloor \frac{t+1}{2} \right\rfloor + d - (t+1)$ *dominant terms with respect to some non-Archimedean absolute value.*

Proof. Suppose at least $t+1$ terms are dominant with respect to every Archimedean absolute value. Let r be the number of distinct characteristic roots of the largest modulus, i.e.

$$|\lambda_1| = \cdots = |\lambda_r| > |\lambda_{r+1}| \geq \cdots \geq |\lambda_s|.$$

Then there are at least $t+1$ terms with bases $\lambda_1, \ldots, \lambda_r$. We denote the number of such terms by T. By Theorem 11 there is an absolute value $|\cdot|_v$ with respect to which at most $\left\lfloor \frac{T}{2} \right\rfloor$ terms with bases among $\lambda_1, \ldots, \lambda_r$ are dominant for $|\cdot|_v$. Therefore, the number of all dominant terms is bounded from above by $\left\lfloor \frac{T}{2} \right\rfloor + d - T$. This expression attains its maximum (provided $T \geq t+1$) at $T = t+1$, thus there are at most $\left\lfloor \frac{t+1}{2} \right\rfloor + d - (t+1)$ terms dominant with respect to $|\cdot|_v$.

The assumption $d < 2t + 2 - \left\lfloor \frac{t+1}{2} \right\rfloor$ is equivalent to $\left\lfloor \frac{t+1}{2} \right\rfloor + d - (t+1) < t+1$, and so there are at most t dominant terms with respect to $|\cdot|_v$. We conclude from this that $|\cdot|_v$ is non-Archimedean. ◀

▶ **Theorem 18.** $\textsc{SimSkolem}(6, 2)$ *is MSTV-reducible.*

Proof. Let $\{u^{(1)}, u^{(2)}\}$ be an instance of $\textsc{SimSkolem}(6, 2)$. From Corollary 17 there is an absolute value $|\cdot|_v$ such that one of the following holds:

1. $|\cdot|_v$ is Archimedean and at most 4 terms are $|\cdot|_v$-dominant,
2. $|\cdot|_v$ is non-Archimedean and at most 3 terms are $|\cdot|_v$-dominant.

In fact, we may assume both $u^{(1)}, u^{(2)}$ have exactly 4 dominant terms if (1) is the case, and exactly 3 dominant terms if (2) is the case; otherwise one of $u^{(1)}, u^{(2)}$ would be in the MSTV class, which immediately yields MSTV-reducibility of the instance.

Case (1). $|\cdot|_v$ is Archimedean with exactly 4 dominant terms in $u^{(1)}, u^{(2)}$.

The associated vectors $\boldsymbol{u}^{(1)}$ and $\boldsymbol{u}^{(2)}$ span a subspace $C \subset \overline{\mathbb{Q}}^6$ where $\dim C = 2$. By Lemma 14 there exists $\boldsymbol{w} \in C$ such that either $\pi_v(\boldsymbol{w}) = \boldsymbol{0}$ or $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 3$. If $\pi_v(\boldsymbol{w}) = \boldsymbol{0}$, the sequence w associated with $\boldsymbol{w}$ has order at most 2. If $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 3$, then w has at most 3 dominant terms with respect to the Archimedean $|\cdot|_v$. In both cases w is in the MSTV class.

Case (2). $|\cdot|_v$ is non-Archimedean with exactly 3 dominant terms in $u^{(1)}, u^{(2)}$.

Applying Lemma 14 again, we find $\boldsymbol{w} \in C$ such that either $\pi_v(\boldsymbol{w}) = \mathbf{0}$ or $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 2$. In the former case, the sequence w associated with $\boldsymbol{w}$ has order at most 3. In the latter case, w has at most 2 dominant terms with respect to the non-Archimedean $|\cdot|_v$. In both cases w is in the MSTV class. ◀

▶ **Theorem 19.** $\textsc{SimSkolem}(9,4)$ *is MSTV-reducible.*

Proof. Let $\{u^{(1)}, u^{(2)}, u^{(3)}, u^{(4)}\}$ be an instance of $\textsc{SimSkolem}(9,4)$. From Corollary 17 there exists either an Archimedean absolute value with at most 6 dominant terms or a non-Archimedean absolute value with at most 5 dominant terms appearing in the LRS $u^{(1)}, \ldots, u^{(4)}$.

Case (1). Assume first that $|\cdot|_v$ is an Archimedean absolute value with $\ell \leq 6$ dominant terms. The associated vectors $\boldsymbol{u}^{(i)}$, $1 \leq i \leq 4$, span a four-dimensional subspace C of $\overline{\mathbb{Q}}^9$, and its projection $\pi_v(C)$ has dimension r. By Lemma 14, if $\ell - r + 1 \leq 3$, then there exists $\boldsymbol{w} \in C$ such that $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 3$. Then the proof is concluded as w lies in the MSTV class. We discuss the situation when $\ell - r + 1 \geq 4$. Since $\ell \leq 6$, we have $r \leq 3$. Note also that we only consider $\ell \geq 4$, as $u^{(1)}$ is in the MSTV class otherwise. Recall also from Lemma 14 that there exist $4 - r$ linearly independent vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{4-r}$ such that $\boldsymbol{w}_i \in C$ with $\pi_v(\boldsymbol{w}_i) = \mathbf{0}$. The problem thus reduces to an instance of a $\textsc{SimSkolem}(9-\ell, 4-r)$. By carefully analysing the possible values of ℓ and r, it is easy to see that all these problems are in the MSTV class.

Case (2). Now we can assume that there exists a non-Archimedean absolute value $|\cdot|_v$ with $\ell \leq 5$ dominant terms. Then, similarly to the Archimedean case, we first note that $\ell - r + 1 \leq 2$ implies the existence of $\boldsymbol{w} \in C$ with $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 2$ whose associated sequence w lies in the MSTV class.

We thus assume $\ell - r + 1 \geq 3$, as well as $\ell \geq 3$. As before, we deduce $r \leq 3$ and again by Lemma 14 the problem can always be reduced to a $\textsc{SimSkolem}(9-\ell, 4-r)$ instance. All these instances are MSTV-reducible since $9 - \ell - (4 - r) = 6 - (\ell - r + 1) \leq 3$ and we can apply Corollary 16. ◀

▶ **Theorem 20.** $\textsc{SimSkolem}(12,6)$ *is MSTV-reducible.*

Proof. Let $\{u^{(1)}, u^{(2)}, \ldots, u^{(6)}\}$ be an instance of $\textsc{SimSkolem}(12,6)$ with characteristic roots $\lambda_1, \ldots, \lambda_s$, where $s \leq 12$.

Case (1). Assume first that $|\cdot|_v$ is an Archimedean absolute value with $\ell \leq 8$ dominant terms appearing in $u^{(1)}, \ldots, u^{(6)}$. We denote by $\pi_v(C)$ the projection to the $|\cdot|_v$-dominant terms of the subspace $C \subseteq \overline{\mathbb{Q}}^{12}$ spanned by the associated vectors of 6 sequences. It has dimension $r \leq \min\{\ell, 6\}$. Similar to the proofs of Theorems 18 and 19, the existence of a linear combination of $\{u^{(i)} : 1 \leq i \leq 6\}$ that lies in the MSTV class is guaranteed in each of the following cases:

- $\ell - r + 1 \leq 3$: then, by Lemma 14, there exists $\boldsymbol{w} \in C$ such that $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 3$. This implies that the associated sequence is in the MSTV class.
- $\ell - r + 1 \geq 4$: now, by Lemma 14 we can find $6-r$ linearly independent vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{6-r}$ such that $\boldsymbol{w}_i \in C$ with $\pi_v(\boldsymbol{w}_i) = \mathbf{0}$. By considering $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{6-r}$, the problem reduces to an instance of $\textsc{SimSkolem}(12-\ell, 6-r)$. Now, by our assumption, $(12 - \ell) - (6 - r) = 6 - \ell + r = -(\ell - r + 1) + 7 \leq 3$. Therefore, each of these $\textsc{SimSkolem}(12-\ell, 6-r)$ instances is MSTV-reducible by Corollary 16.

Case (2a): If $\ell \leq 6$ terms are dominant with respect to a non-Archimedean absolute value $|\cdot|_v$, then we can proceed similarly:

- $\ell - r + 1 \leq 2$: then, by Lemma 14, there exists $\boldsymbol{w} \in C$ such that $1 \leq \#\operatorname{supp}(\pi_v(\boldsymbol{w})) \leq 2$. This implies that the associated sequence is in the MSTV class.
- $\ell - r + 1 \geq 3$: by Lemma 14 we can find $6 - r$ linearly independent vectors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{6-r}$ such that $\boldsymbol{w}_i \in C$ with $\pi_v(\boldsymbol{w}_i) = \boldsymbol{0}$. By eliminating the $|\cdot|_v$-dominant terms, the problem reduces to an instance of a SimSkolem$(12-\ell, 6-r)$. Moreover, $(12-\ell)-(6-r) = 6-\ell+r = -(\ell-r+1)+7 \leq 4$. The new case is when $12-\ell-(6-r) = 4$. Due to $12-\ell \geq 6$, these instances are MSTV-reducible from Theorem 18 and Lemma 15. All other SimSkolem$(12-\ell, 6-r)$ instances we obtain are MSTV-reducible by Corollary 16.

However, we now come to the first case that requires further analysis. Assume now that there are at least 9 dominant terms for every Archimedean absolute value. By Corollary 17 (setting $t := 8$) we are guaranteed that there are at most 7 dominant terms with respect to some non-Archimedean absolute value.

Case (2b): We have already considered the case of at most 6 dominant terms; hence we proceed under the assumption that $|\cdot|_{\mathfrak{p}}$ is the non-Archimedean absolute value with exactly 7 dominant terms constructed as in Corollary 17.

Let m denote the number of distinct characteristic roots with the largest modulus, without loss of generality,

$$|\lambda_1| = \cdots = |\lambda_m| > |\lambda_{m+1}| \geq \cdots \geq |\lambda_s|\,.$$

Let $T \in \{9, 10, 11, 12\}$ be the number of terms associated with $\lambda_1, \ldots, \lambda_m$. Since there are exactly 7 dominant terms with respect to $|\cdot|_{\mathfrak{p}}$, and since there are at most $\lfloor \frac{T}{2} \rfloor$ of them associated with $\lambda_1, \ldots, \lambda_m$[11], it is easy to see that only two cases are possible. Either $T = 9$ and exactly 3 terms with bases among $\lambda_{m+1}, \ldots, \lambda_s$ are $|\cdot|_{\mathfrak{p}}$-dominant. Or $T = 10$ and exactly 2 terms with bases among $\lambda_{m+1}, \ldots, \lambda_s$ are $|\cdot|_{\mathfrak{p}}$-dominant. Crucially, in both cases all terms with bases among $\lambda_{m+1}, \ldots, \lambda_s$ are $|\cdot|_{\mathfrak{p}}$-dominant.

We now employ Lemma 14 for $|\cdot|_{\mathfrak{p}}$. Let the projection $\pi_{\mathfrak{p}}(C)$ to the $|\cdot|_{\mathfrak{p}}$-dominant terms have dimension r. If $r = 6$, then we have $7 - r + 1 = 2$, and so there exists $\boldsymbol{w} \in C$ such that $1 \leq \#\operatorname{supp}(\pi_{\mathfrak{p}}(\boldsymbol{w})) \leq 2$. Then, the associated sequence is in the MSTV class. Otherwise, if $r \leq 5$, we can find $\boldsymbol{w} \in C$ such that $\#\operatorname{supp}(\pi_{\mathfrak{p}}(\boldsymbol{w})) = 0$. Recall from the previous paragraph that $\operatorname{supp}(\pi_{\mathfrak{p}}(\boldsymbol{w}))$ contains no components that correspond to terms with bases $\lambda_{m+1}, \ldots, \lambda_s$. In other words, the associated sequence of $\boldsymbol{w}$ has at most 5 non-zero terms, all of them having bases of the same modulus $|\lambda_1|$. By Theorem 11, there exists an absolute value for which at most 2 of these terms are dominant, placing this sequence in the MSTV class. ◀

These theorems show that Orbit(d,t) is decidable for $(d,t) = (6,4)$, $(9,5)$, and $(12,6)$. Furthermore, those are the smallest d for which Orbit(d,t) with, respectively, $t = 4,5,6$ can be decided using the properties of the MSTV class.

By Corollary 17, the inequality

$$d \leq 2k + 4 - \left\lfloor \frac{k+3}{2} \right\rfloor \tag{3.3}$$

implies that either there exists an Archimedean absolute value $|\cdot|_v$ with at most $k+2$ dominant terms, or there is a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$ such that the absolute value $|\cdot|_{\mathfrak{p}}$ has at most $k+1$ dominant terms.

[11] Recall that in Corollary 17, the dominant terms are constructed by applying Theorem 11 to $\lambda_1, \ldots, \lambda_m$.

The condition (3.3) is optimal, as witnessed by the following family of examples. In particular, it is easy to see that SimSkolem with (5,1), (8,3) and (11,5) are not MSTV-reducible.

▶ **Example 21.** Given integers d, k such that

$$d > 2k + 4 - \left\lfloor \frac{k+3}{2} \right\rfloor , \tag{3.4}$$

we show instances of SimSkolem(d, k) that are not MSTV-reducible.

First, we consider odd k; that is, the case where $k + 3$ is even. Let $s \coloneqq (k + 3)/2$ and notice that $d - s > k + 1$ follows. Let Λ_{2s} be as defined in Example 12. Let $\lambda_{s+1}, \dots, \lambda_{d-s}$ be Gaussian primes[12] smaller in modulus than any prime factor of λ_i with $1 \le i \le s$. We choose d characteristic roots $\Lambda_{2s} \cup \{\lambda_{s+1}, \dots, \lambda_{d-s}\}$.

Using the argument of Example 12, we see that for every Archimedean absolute value the dominant roots are $\lambda_1, \dots, \lambda_s, \overline{\lambda}_1, \dots, \overline{\lambda}_s$, that is, there are $2s = k + 3$ dominant roots. Among non-Archimedean absolute values, we identify the absolute values $|\cdot|_p$ where p is a prime factor of some element in Λ_{2s}. For each of them, there are $s + d - 2s \ge k + 2$ dominant roots. Moreover, for the absolute values $|\cdot|_{\lambda_i}$ with $i \ge s + 1$, there are $d - 1$ dominant terms, and for all other non-Archimedean absolute values all d roots are dominant.

Now we choose our k LRS as $u_n^{(1)}, \dots, u_n^{(k)}$ with

$$u_n^{(i)} = \sum_{j=1}^{s} j^{i-1} \lambda_j^n + \sum_{j=1}^{s} (j+s)^{i-1} \overline{\lambda}_j^n + \sum_{j=s+1}^{d-s} (j+s)^{i-1} \lambda_j^n \,.$$

Let $|\cdot|_v$ be an arbitrary absolute value and let ℓ denote the number of dominant roots with respect to it. Denote by $C \subseteq \overline{\mathbb{Q}}^d$ the vector subspace spanned by the associated vectors of $u^{(1)}, \dots, u^{(k)}$. We show that $\#\operatorname{supp}(\pi_v(\boldsymbol{w})) \ge \ell - (k-1)$ for any non-zero vector $\boldsymbol{w} \in C$. Indeed, assume that among components that correspond to $|\cdot|_v$-dominant roots there are k components $I = \{i_1, \dots, i_k\}$ such that for some $\boldsymbol{w} \ne \boldsymbol{0}$ we have $\boldsymbol{w}_i = 0$ for all $i \in I$. Then $\boldsymbol{u}^{(1)}, \dots, \boldsymbol{u}^{(k)}$ restricted to components in I are linearly dependent; yet these vectors constitute a $k \times k$ Vandermonde matrix $V(i_1, \dots, i_k)$ whose determinant is non-zero, which is a contradiction.

Consequently, there is no linear combination of the LRS with at most 3 Archimedean dominant roots or at most 2 non-Archimedean dominant roots, so this (d, k)-instance is not MSTV-reducible.

We now prove that some SimSkolem(d, k) instances that satisfy (3.4) are not MSTV-reducible, *for all even k as well.* Assume that for some even k there exists d as in (3.4) such that SimSkolem(d, k) is MSTV-reducible. From Equation (3.4) we have

$$d + 1 > 2k + 4 - \left\lfloor \frac{k+3}{2} \right\rfloor + 1 = 2(k+1) + 4 - \left\lfloor \frac{(k+1)+3}{2} \right\rfloor ,$$

and therefore, SimSkolem$(d + 1, k + 1)$ is MSTV-reducible by Lemma 15. This contradicts what we have just proved about the odd k case.

We will now show that for every parameter $d - k$ there exists sufficiently large d such that SimSkolem(d, k) is MSTV-reducible. This is most naturally formulated in terms of the reduced Subspace Orbit Problem: for every target dimension t there exists d such that Orbit(d, t) is MSTV-reducible, and hence is decidable.

[12] As before, chosen so that they are not associates to each other or their conjugates.

▶ **Theorem 2.** *$\textsc{SimSkolem}(d,k)$ is decidable for all (d,k) satisfying $d-k \leq 2\log_3 d$. Equivalently, $\textsc{Orbit}(d,t)$ is decidable whenever $t \leq 2\log_3 d$.*

Proof. We have shown the statement for all $t \leq 6$. Suppose that $t \geq 7$ and that the theorem has been proven for every target dimension smaller than t. Pick d,k such that $d-k=t$ and $d-k \leq 2\log_3 d$, and consider an arbitrary instance of $\textsc{SimSkolem}(d,k)$. Notice that for $d-k \geq 7$ we have $d-k < 3^{\frac{d-k}{2}-1}$, and so $\frac{d}{3} \geq 3^{\frac{d-k}{2}-1} > d-k$. This implies $k > \frac{2d}{3}$.

We apply Corollary 17 with a parameter $\frac{2d}{3}$, from which we argue that there exists an absolute value $|\cdot|_v$ with $\ell \leq \frac{2d}{3}$ dominant terms, either Archimedean or not. We can now apply Lemma 14 for the subspace $C \subseteq \overline{\mathbb{Q}}^d$ spanned by k vectors of our sequences. Let $r := \dim \pi_v(C)$. Notice that $r \leq \min\{\ell,k\} = \ell$. If $\ell - r \in \{0,1\}$, then by Lemma 14 there exists a sequence with at most 2 $|\cdot|_v$-dominant terms. Therefore, the problem is MSTV-reducible.

We now assume that $\ell - r \geq 2$. Since $k-r \geq 1$, we deduce from Lemma 14 that this instance reduces to $\textsc{SimSkolem}(d-\ell,k-r)$ by eliminating the $|\cdot|_v$-dominant terms. Notice that $d-\ell-(k-r) \leq d-k-2$ by our latest assumption. Moreover,

$$\ell \leq \frac{2d}{3} \Leftrightarrow d-\ell \geq \frac{d}{3} \Rightarrow d-\ell \geq 3^{\frac{d-k}{2}-1} = 3^{\frac{d-k-2}{2}},$$

so we have $d-\ell \geq 3^{\frac{d-\ell-(k-r)}{2}}$. The problem we reduced to has a strictly smaller target dimension, as $d-\ell-(k-r) < d-k$ follows from $\ell - r \geq 2$. Consequently, $\textsc{SimSkolem}(d-\ell,k-r)$ is MSTV-reducible by induction on target dimension. ◀

4 Hardness

In this section we show that if for some $C \in (0,1)$ there is an algorithm to decide $\textsc{Orbit}(d,t)$ for all t,d such that $t \leq Cd$, then the Skolem Problem is decidable.

Given a $\overline{\mathbb{Q}}$-LRS u, pick multiplicatively independent algebraic numbers $\mu_1,\ldots,\mu_s \neq 0$ such that we may write

$$u_n = L(\mu_1^n,\ldots,\mu_s^n) \cdot P(n+1,\mu_1^n,\ldots,\mu_s^n)$$

for some Laurent monomial $L(x_1,\ldots,x_s)$ and some polynomial $P(x_0,\ldots,x_s)$ with algebraic coefficients (let x_0 correspond to $n+1$ and x_i correspond to μ_i^n).[13] Note that monomials of P correspond to terms in the exponential polynomial representation of u. Note also that $u_n = 0$ if and only if $P(n+1,\mu_1^n,\ldots,\mu_s^n) = 0$. We want to find polynomials $Q_1,\ldots,Q_k$ such that the LRS defined by $Q_1P,\ldots,Q_kP$ form an instance of $\textsc{SimSkolem}(d,k)$ with d small compared to k.

▶ **Lemma 22.** *Given a non-degenerate LRS u with associated polynomial $P(x_0,\ldots,x_s)$, there exists a family of $\textsc{SimSkolem}$ instances $I_1,I_2,\ldots$ such that each I_ℓ consists of $k=\ell^{s+1}$ non-degenerate LRS that satisfy a recurrence relation of order $d \leq \ell^{s+1}+B\ell^s$ for a constant B that only depends on P. Moreover, the set of simultaneous zeros $\mathcal{Z}(I_\ell)$ is equal to $\mathcal{Z}(u)$.*

Proof. We will identify monomials $x_0^{m_0}x_1^{m_1}\ldots x_s^{m_s}$ with points in $\mathbb{Z}^{s+1}$ by

$$x_0^{m_0}x_1^{m_1}\ldots x_s^{m_s} \mapsto (m_0,m_1,\ldots,m_s)\,.$$

[13] The μ_i are not necessarily the characteristic roots of u because one may need to take roots. For example if there is a multiplicative relation $\lambda_1^3 = \lambda_2^2$, one can take $\mu_1 = \lambda_1^{1/2}$, for some definition of $\lambda_1^{1/2}$.

Let R be the set of points $(m_0, m_1, \dots, m_s)$ such that P has a term $x_0^\nu x_1^{m_1} \dots x_s^{m_s}$ for $0 \le m_0 \le \nu$.[14]

We fix an arbitrary integer ℓ and construct the instance I_ℓ. Let

$$C_\ell = \{(m_0, m_1, \dots, m_s) \in \mathbb{Z}^{s+1} : 0 \le m_i \le \ell - 1\}.$$

Let $k = \ell^{s+1} = |C_\ell|$, and let $Q_1, \dots, Q_k$ be the monomials represented by each point in C_ℓ. Let T be the set of monomials present in $Q_1P, \dots, Q_kP$. Consider the Minkowski sum

$$R + C_\ell = \{\boldsymbol{x} + \boldsymbol{y} : \boldsymbol{x} \in R,\ \boldsymbol{y} \in C_\ell\}.$$

We have $T \subseteq R + C_\ell \subseteq C_{\ell+r}$ where r is the largest component of any point of R.

We now view Q_iP, $1 \le i \le k$, as LRS by assigning $x_0 = n + 1$ as well as $x_j = \mu_j^n$ for all $1 \le j \le s$. They constitute I_ℓ. These k LRS are linearly independent. Indeed, their linear dependence would imply linear dependence of the LRS $u_n^{(i)} = Q_i(n + 1, \mu_1^n, \dots, \mu_s^n)$, which is impossible as each $u_n^{(i)} = (n + 1)^{m_0} \mu_1^{m_1 n} \dots \mu_s^{m_s n}$ for distinct tuples $(m_0, \dots, m_s)$. The LRS corresponding to $Q_1P, \dots, Q_kP$ thus form a $\textsc{SimSkolem}(d, k)$ instance with

$$d \le |T| \le |R + C_\ell| \le |C_{\ell+r}| = (\ell + r)^{s+1} \le \ell^{s+1} + B\ell^s,$$

where B is a constant depending only on r and s. Note that the quotients of distinct characteristic roots of the LRS are not roots of unity since such quotients are always Laurent monomials of the μ_i. Indeed, let $\mu_1^{t_1} \dots \mu_s^{t_s}$ for $t_1, \dots, t_s \in \mathbb{Z}$ be a root of unity of order $m > 0$. Then $(mt_1, \dots, mt_s)$ needs to be a multiplicative relation of $\mu_1, \dots, \mu_s$ contradicting our assumption.

Since $Q_i(n + 1, \mu_1^n, \dots, \mu_s^n) \ne 0$ for all $1 \le i \le k$, $n \in \mathbb{N}$, the set of simultaneous zeros $\mathcal{Z}(I_\ell)$ is exactly the set of n such that $P(n + 1, \mu_1^n, \dots, \mu_s^n) = 0$. Therefore, it is exactly the set $\mathcal{Z}(u)$. ◀

So, for k arbitrarily large, the Skolem Problem on u reduces to $\textsc{SimSkolem}(\tilde{d}, k)$ with

$$\tilde{d} \le k + Bk^{\frac{s}{s+1}},$$

for some constant B depending on u, by solving an instance given by Lemma 22 to decide if $\mathcal{Z}(u) \ne \varnothing$. Therefore, if $\textsc{SimSkolem}(d, k)$ is decidable for some $d \ge k + Bk^{\frac{s}{s+1}} \ge \tilde{d}$, then one can determine whether $\mathcal{Z}(u)$ is non-empty. This is employed in the proof of the hardness result next.

▶ **Theorem 23.** *If there exists $C \in (0, 1)$ such that $\textsc{Orbit}(d, t)$ is decidable for all (d, t) that satisfy $t \le Cd$, then the Skolem Problem is decidable.*

Proof. Under the hypothesis, $\textsc{SimSkolem}(d, k)$ is decidable for all $d \ge \frac{1}{C}(d - k)$ by Proposition 8. We now use this to decide for any non-degenerate LRS u whether $\mathcal{Z}(u) \ne \varnothing$. Given u with a polynomial $P(x_0, \dots, x_s)$, we shall find $d \ge k > 0$ such that

$$\frac{1}{C}(d - k) \le d \tag{4.1}$$

while some instance of $\textsc{SimSkolem}(d, k)$ encodes the Skolem Problem for u. As in Lemma 22, consider $k = \ell^{s+1}$ as ℓ increases, and recall the constant B defined ibid. We set $d := \ell^{s+1} + B\ell^s$. In order to satisfy (4.1), we choose $\ell \ge \frac{1-C}{C}B$ as we can take ℓ arbitrary large.

$\textsc{SimSkolem}(d, k)$ is decidable by the hypothesis of the theorem. Let $\tilde{d}$ be the order of the LRS in the instance I_ℓ constructed in Lemma 22. By construction, $d \ge \tilde{d}$ and so $\textsc{SimSkolem}(\tilde{d}, k)$ is decidable, too. We can thus answer whether $\mathcal{Z}(u) \ne \varnothing$. ◀

[14] This different treatment of x_0 is necessary due to the difference in how powers of n affect the order of an LRS.

5 Complexity

In this section, we will prove complexity upper bounds on the reduced Subspace Orbit Problem in the MSTV-reducible cases we have identified.

We emphasise that unlike in previous sections, we consider $\text{ORBIT}_{\mathbb{K}}$ over the field $\mathbb{K} = \mathbb{Q}$. Our input I will be a matrix $M \in \mathbb{Q}^{d\times d}$ such that no ratio of distinct eigenvalues of M is a root of unity, an initial vector $\boldsymbol{x} \in \mathbb{Q}^d$, and a linearly independent set of rational vectors $\{\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(t)}\}$ spanning a target subspace $S \subseteq \mathbb{Q}^d$. Let $\|I\|$ measure the bit-size of an input I.

Recall from Section 1 that an input to $\text{SIMSKOLEM}_{\mathbb{Q}}(d,k)$ is k linearly independent, non-degenerate LRS $\{u^{(1)}, \ldots, u^{(k)}\}$ satisfying the same recurrence relation of order d; we assume the input is structured as a vector of rational coefficients of the recurrence relation, along with k rational vectors of initial values. We denote the sum of their bit-sizes by $\|(u^{(1)}, \ldots, u^{(k)})\|$.

The notation $\mathsf{poly}(x)$ will denote any quantity bounded above by $x^{O(1)}$, and $2^{\mathsf{poly}(x)}$ any quantity bounded above by $2^{x^{O(1)}}$.

To decide $\text{ORBIT}_{\mathbb{Q}}(d,t)$ with $t \le 2\log_3 d$, we proceed as follows:

Steps 1. Show that $\text{ORBIT}_{\mathbb{Q}}$ on $(M, \boldsymbol{x}, S)$ reduces to $\text{SIMSKOLEM}_{\mathbb{Q}}$ on $u^{(1)}, \ldots, u^{(k)}$ such that $\|(u^{(1)}, \ldots, u^{(k)})\| = \mathsf{poly}(\|(M, \boldsymbol{x}, S)\|)$.

Steps 2. If there is a linear combination of the LRS $u^{(i)}$ that lies in the MSTV class, then such a linear combination exists, whose coefficients (of the exponential polynomial form (2.3)) have bounded degree and height.

Steps 3. Apply bounds on the zeros of non-degenerate LRS in the MSTV class to prove upper bounds on the simultaneous zeros of $u^{(1)}, \ldots, u^{(k)}$.

We note that Steps 1–3 as listed justify the correctness of Corollary 34, which provides an effective upper bound on the solutions n to $\text{ORBIT}_{\mathbb{Q}}$. The actual decision procedure amounts to the "guess and check" described in the proof of Theorem 35. To this end, our complexity results require neither finding the sequences $u^{(i)}$ (Step 1), nor explicitly computing an MSTV sequence (Step 2).

For Step 1, the reduction from $\text{ORBIT}_{\mathbb{Q}}$ to $\text{SIMSKOLEM}_{\mathbb{Q}}$, we need to prove that there is a basis of $S^{\perp}$ which is not too large. We use a version of Siegel's lemma, by Bombieri and Vaaler [12, Theorem 2].

▶ **Theorem 24.** *Let $A \in \mathbb{Z}^{m\times n}$ be a matrix with $n > m$, whose rows are linearly independent. Suppose $|a_{ij}| < B$ for all $1 \le i \le m$ and $1 \le j \le n$. Then there are $n-m$ linearly independent integral solutions $\boldsymbol{x}^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})^{\top}$ to $A\boldsymbol{x} = 0$ such that*

$$\prod_{i=1}^{n-m} \max_j |x_j^{(i)}| \le G^{-1}\sqrt{|\det(AA^{\top})|},$$

where G is the greatest common divisor of all the $m \times m$ minors of A.

▶ **Lemma 25.** *Let S be a subspace of $\mathbb{Q}^d$ with $\dim S = d-k$. There is a basis $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(k)} \in \mathbb{Q}^d$ of $S^{\perp}$ such that $\|\boldsymbol{w}^{(i)}\| = \mathsf{poly}(\|S\|)$.*

Proof. S is specified by a set of linearly independent rational vectors $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(t)} \in \mathbb{Q}^d$, where $t = d-k$. The lowest common multiple L of the denominators of all the entries has modulus at most $2^{dt\|S\|}$. Let A be an integral $t \times d$ matrix whose rows are $L\boldsymbol{v}^{(1)}, \ldots, L\boldsymbol{v}^{(t)}$. By Theorem 24, there are $d-t$ linearly independent integral solutions $\boldsymbol{w}^{(1)}, \ldots, \boldsymbol{w}^{(d-t)}$ to $A\boldsymbol{x} = 0$ that satisfy

$$\prod_{i=1}^{d-t} \max_j |w_j^{(i)}| \le \sqrt{|\det(AA^\top)|}\,.$$

Then $\boldsymbol{w}^{(1)}, \dots, \boldsymbol{w}^{(d-t)}$ is exactly a basis of $S^\perp$. It remains to show

$$\sqrt{|\det(AA^\top)|} \le 2^{\mathsf{poly}(\|S\|)}$$

to get the claimed result. By Hadamard's inequality,

$$\begin{aligned} |\det(AA^\top)| &\le (\max_{i,j} |(AA^\top)_{ij}|)^t t^{t/2} \le (d \max_{i,j} |A_{ij}|^2)^t t^{t/2} \\ &\le (dL^2)^t (\max_{i,j} |v_j^{(i)}|)^{2t} t^{t/2} = 2^{\mathsf{poly}(\|S\|)}\,. \end{aligned}$$ ◀

▶ **Lemma 26.** *The characteristic polynomial g_A of a matrix $A \in \mathbb{Q}^{d\times d}$ has coefficients of bit size* $\mathsf{poly}(\|A\|)$.

Proof. First, write $A = \frac{1}{a}B$, where B has entries in $\mathbb{Z}$, noting we can choose $a \neq 0$ such that $\|a\|, \|B\| = \mathsf{poly}(\|A\|)$. Let $g_B(x) = x^d + c_1 x^{d-1} + \cdots + c_d$. If $J \subseteq \{1, \dots, d\}$ then let B_J denote the principal submatrix formed of rows and columns with indices in J. Then the coefficients c_r may be expressed as a sum of principal minors of B (see e.g. [30, p.294]) as

$$c_r = \sum_{|J|=r} (-1)^r \det(B_J)\,.$$

Write $B = (b_{ij})_{1\le i,j\le d}$. There are $\binom{d}{r}$ many $r \times r$ principal minors of A so by Hadamard's inequality applied to B_J we get

$$|c_r| \le \binom{d}{r} \left(\max_{1\le i,j\le d} |b_{ij}|\right)^r r^{r/2} \le d! \|B\|^d d^{d/2}$$

and therefore $\|c_r\| = \mathsf{poly}(\|A\|)$. Now note that $g_B(a \cdot A) = 0$ and after dividing by a^d, it is easy to see that $g_A(x)$ is

$$g_A(x) = x^d + \frac{c_1}{a} x^{d-1} + \cdots + \frac{c_d}{a^d}\,,$$

so indeed every coefficient c_r/a^r, $1 \le r \le d$, has bit-size $\mathsf{poly}(\|A\|)$, since $\|a\|, \|c_r\| = \mathsf{poly}(\|A\|)$, for all $1 \le r \le d$. ◀

The proposition below refines a reduction from Proposition 8.

▶ **Proposition 27.** $\textsc{Orbit}_\mathbb{Q}$ *on* $(M, \boldsymbol{x}, S)$ *reduces to* $\textsc{SimSkolem}_\mathbb{Q}$ *on* $u^{(1)}, \dots, u^{(k)}$*, for* $\|(u^{(1)}, \dots, u^{(k)})\| = \mathsf{poly}(\|(M, \boldsymbol{x}, S)\|)$.

Proof. Let $\boldsymbol{w}^{(1)}, \dots, \boldsymbol{w}^{(k)}$ be a basis for $S^\perp$. Then $\textsc{Orbit}_\mathbb{Q}$ on $(M, \boldsymbol{x}, S)$ reduces to $\textsc{SimSkolem}_\mathbb{Q}$ on the LRS $u_n^{(i)} = (\boldsymbol{w}^{(i)})^\top M^n \boldsymbol{x}$ for $1 \le i \le k$ (see Proposition 8). By Lemma 25, we have a basis of $S^\perp$ such that $\|\boldsymbol{w}^{(i)}\| = \mathsf{poly}(\|S\|)$ for all i, so we may bound the initial values $\|u_n^{(i)}\| = \mathsf{poly}(\|(M, \boldsymbol{x}, S)\|)$ for each $0 \le n \le d-1$ and $1 \le i \le k$. Also, the characteristic polynomial of M is exactly the characteristic polynomial of a recurrence relation $(c_1, \dots, c_d) \in \mathbb{Q}^d$ satisfied by each $u^{(i)}$, so by Lemma 26, we have $\|u^{(i)}\| = \mathsf{poly}(\|(M, \boldsymbol{x}, S)\|)$. ◀

We have completed Step 1. Next, we discuss the exponential polynomial form (2.3) of the LRS, and so we need to bound the heights and degrees of the coefficients and characteristic roots.

▶ **Proposition 28.** *Given an order-d $\mathbb{Q}$-LRS $u = \sum_{i,j} c_{i,j} n^j \lambda_i^n$, we have $h(c_{i,j}), h(\lambda_i) = \mathsf{poly}(\|u\|)$, and $\deg(\lambda_i) \le d$ and $c_{i,j} \in \mathbb{Q}(\lambda_i)$.*

Proof. Since λ_i is a root of the characteristic polynomial

$$g(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$$

of u, where $a_i \in \mathbb{Z}$, we have $\deg \lambda_i \le d$. Furthermore, let $f(x) = b_r x^r + \cdots + b_0$ be the minimal polynomial of λ, and let $H(\lambda)$ denote the “naïve height” of λ, defined by $H(\lambda) = \max\{|b_0|, \dots, |b_r|\}$. Then, since f divides g, by [39, Lemma 3.11 and Remark 2, p. 81] we have

$$\begin{aligned} h(\lambda_i) &\le \frac{1}{r} \log H(\lambda_i) + \frac{1}{2r} \log(r+1) \\ &\le \frac{1}{r} \log\left(2^d \sqrt{d+1} H(g)\right) + \frac{1}{2r} \log(r+1) \\ &= \mathsf{poly}(\|u\|) \,. \end{aligned}$$

Now, by [1, Lemma 6], we have $c_{i,j} = q_0 + q_1\lambda_i + \cdots + q_{d-1}\lambda_i^{d-1}$ for rationals $|q_i| \le 2^{\mathsf{poly}(\|u\|)}$. Therefore, using Proposition 7,

$$h(c_{i,j}) \le \log d + \sum_{s=0}^{d-1} h(q_s) + \sum_{s=0}^{d-1} s h(\lambda_i) = \mathsf{poly}(\|u\|)$$

holds as well as $\deg(c_{i,j}) \le d$. ◀

We proceed with Step 2 of our analysis: if there is a linear combination of $u^{(1)}, \dots, u^{(k)}$ lying in the MSTV class, then such a linear combination exists of small height and degree. First, we have a lemma that allows us to restrict ourselves to kernels of dimension 1, which simplifies the proof. Essentially, the lemma says that if one has a linear combination in the MSTV class with minimal support amongst linear combinations in the MSTV class, then in fact the support is minimal amongst all linear combinations in general.

▶ **Lemma 29.** *Let C be the span over $\overline{\mathbb{Q}}$ of $\boldsymbol{u}^{(1)}, \dots, \boldsymbol{u}^{(k)} \in \overline{\mathbb{Q}}^d$, the vectors representing the LRS $u^{(1)}, \dots, u^{(k)}$. Suppose that $\boldsymbol{u} \in C$ represents an LRS in the MSTV class and has a minimal support among such vectors in C; that is, if $\boldsymbol{u}' \in C$ represents an LRS in the MSTV class then $\operatorname{supp}(\boldsymbol{u}') \subsetneq \operatorname{supp}(\boldsymbol{u})$ implies $\boldsymbol{u}' = \boldsymbol{0}$.*

Then we have $\dim(\ker \pi_{\neg V}|_C) = 1$ where $V = \operatorname{supp}(\boldsymbol{u})$ and $\pi_{\neg V}$ is the projection to the components $\{1, \dots, d\} \setminus V$. That is, any $\boldsymbol{w} \in C$ with $\operatorname{supp}(\boldsymbol{w}) \subseteq \operatorname{supp}(\boldsymbol{u})$ is of the form $\boldsymbol{w} = \eta \boldsymbol{u}$ for some $\eta \in \overline{\mathbb{Q}}$.

Proof. Since $\boldsymbol{u}$ corresponds to an LRS in the MSTV class, it corresponds to an LRS with at most r dominant roots with respect to some absolute value $|\cdot|_v$, where $r \le 2$ if $|\cdot|_v$ is non-Archimedean and $r \le 3$ if $|\cdot|_v$ is Archimedean. Suppose $\operatorname{supp}(\boldsymbol{w}) \subseteq \operatorname{supp}(\boldsymbol{u})$. If $\boldsymbol{w} \neq \eta \boldsymbol{u}$ for any $\eta \in \overline{\mathbb{Q}}$, then we can choose i such that $i \in \operatorname{supp}(\boldsymbol{u})$ corresponds to a $|\cdot|_v$-dominant term, as well as choose $j \neq i$, so that $\frac{w_i}{u_i} \neq \frac{w_j}{u_j}$. Then $\boldsymbol{w}' = \boldsymbol{w} - \frac{w_j}{u_j}\boldsymbol{u}$ has $w_i' \neq 0$ and thus the set of $|\cdot|_v$-dominant terms for $\boldsymbol{w}'$ is a subset of $|\cdot|_v$-dominant terms for $\boldsymbol{w}$. Therefore, the LRS of $\boldsymbol{w}'$ lies in the MSTV class. Moreover, $w_j' = 0$ and so $\operatorname{supp}(\boldsymbol{w}') \subsetneq \operatorname{supp}(\boldsymbol{u})$, which contradicts the fact that $\operatorname{supp}(\boldsymbol{u})$ is minimal and concludes the proof. ◀

This lemma allows us to construct a linear combination in the MSTV class of small height. First, we need an elementary height bound on the determinant of a matrix.

▶ **Lemma 30.** *For a matrix $A = (a_{ij})_{1\le i,j\le m} \in \mathbb{K}^{m\times m}$ over a number field $\mathbb{K}$, we have*

$$h(\det A) \le \frac{m}{2}\log m + m \sum_{1\le i,j\le m} h(a_{ij})\,.$$

The proof is elementary, and follows from Hadamard's inequality and the definition of the height; it may be found in [8, Appendix A.1].

▶ **Lemma 31.** *Suppose there exists $\boldsymbol{\beta} = (\beta_1,\ldots,\beta_k) \in \overline{\mathbb{Q}}^k$ such that $\sum_{i=1}^k \beta_i u^{(i)}$ lies in the MSTV class. Then there exists such a $\boldsymbol{\beta}$ with $h(\beta_i) = \mathsf{poly}(\|u\|)$.*

Proof. If there exists a linear combination in the MSTV class, then certainly there exists a linear combination $\boldsymbol{v}$ with minimal support among linear combinations in the MSTV class. By Lemma 29, if $\mathrm{supp}(\boldsymbol{v}) = V$, then $\dim(\ker \pi_{\neg V}|_C) = 1$: any vector in $\ker \pi_{\neg V}|_C$ is a scalar multiple of $\boldsymbol{v}$ and lies in the MSTV class. Let

$$A = \left(\pi_{\neg V}(\boldsymbol{u}^{(1)}) \mid \cdots \mid \pi_{\neg V}(\boldsymbol{u}^{(k)})\right)\,,$$

then we just need to find $\boldsymbol{\beta}$ such that $A\boldsymbol{\beta} = 0$.

Since $\dim\ker A = 1$, rank $A = k-1$, so we can pick $k-1$ linearly independent rows of A to form a $(k-1)\times k$ matrix B with the same kernel. Let $\beta_i = (-1)^{i+1}\det B^{(i)}$, where $B^{(i)}$ is B with the ith column removed. This is an element of the kernel; indeed, we have by Laplace expansion that for any vector $\boldsymbol{y} = (y_1,\ldots,y_k)^\top \in \overline{\mathbb{Q}}^k$,

$$\det\begin{pmatrix}\boldsymbol{y}^\top\\ B\end{pmatrix} = \sum_{i=1}^k (-1)^{i+1} y_i \det B^{(i)} = \boldsymbol{y}^\top\boldsymbol{\beta}$$

and so $\boldsymbol{y}^\top\boldsymbol{\beta} = 0$ if $\boldsymbol{y}^\top$ is any row of B, so $B\boldsymbol{\beta} = 0$ and hence $A\boldsymbol{\beta} = 0$. Now by Lemma 30, we have $h(\beta_i) = \mathsf{poly}(\|u\|)$, as required. ◀

▶ **Corollary 32.** *Suppose $\boldsymbol{\beta} = (\beta_1,\ldots,\beta_k) \in \overline{\mathbb{Q}}^k$ is such that $\sum_{i=1}^k \beta_i u^{(i)} = \sum_{i=1}^R P_i(n)\lambda_i^n$ lies in the MSTV class and is of minimal support. Let $\mathbb{K} = \mathbb{Q}(\lambda_1,\ldots,\lambda_R)$. Then there exists $\boldsymbol{\gamma} \in \mathbb{K}^k$ such that $\boldsymbol{\gamma} = \eta\boldsymbol{\beta}$ for some $\eta \in \overline{\mathbb{Q}}$ with $h(\boldsymbol{\gamma}) = \mathsf{poly}(\|\boldsymbol{\beta}\|)$.*

The proof of this corollary follows from using the trace to construct $\boldsymbol{\gamma}$; it may be found in [8, Appendix A.2]. In [8, Appendix A.3], the following bound on zeros of LRS is proven.

▶ **Theorem 33.** *Suppose that $u_n = \sum_{i=1}^s P_i(n)\lambda_i^n$, for polynomials P_i of degree at most δ. Let h_P be the largest height of any coefficient of any P_i and let $h_\lambda := \max_{i=1}^s h(\lambda_i)$. Suppose that u is non-degenerate and lies in the MSTV class, that is, there is absolute value $|\cdot|_v$ with*

$$|\lambda_1|_v = \cdots = |\lambda_r|_v > |\lambda_{r+1}|_v \ge \cdots \ge |\lambda_s|_v$$

and $r \le 3$ if $|\cdot|_v$ is Archimedean, and $r \le 2$ if $|\cdot|_v$ is non-Archimedean. Let $\mathbb{K}$ be the number field generated by $\lambda_1,\ldots,\lambda_s$ and the coefficients of $P_1,\ldots,P_s$, and let $D = [\mathbb{K} : \mathbb{Q}]$. Then $u_n = 0$ implies that

$$n < \mathsf{poly}(s)\cdot 2^{\mathsf{poly}(D,h_\lambda,h_P,\delta)}\,.$$

The proof is essentially the same as the decidability proof for LRS in the MSTV class using Baker's theorem [31, 38, 10], but the constants are carried through more precisely to achieve the desired bound ([14, Sections C-F] proves a special case for order ≤ 4 LRS).

As Step 3, we apply this to derive upper bounds on the simultaneous zeros of LRS; and hence on the solutions to $\textsc{Orbit}_{\mathbb{Q}}(d,t)$.

► **Corollary 34.** *If $M \in \mathbb{Q}^{d\times d}$, $\boldsymbol{x} \in \mathbb{Q}^d$ and $S \subseteq \mathbb{Q}^d$ of dimension t define an MSTV-reducible instance of $\textsc{Orbit}_{\mathbb{Q}}(d,t)$, then $M^n\boldsymbol{x} \in S$ implies that $n < 2^{\mathsf{poly}(d^t, \|(M,\boldsymbol{x},S)\|)}$.*

Proof. By combining Propositions 27 and 28, Lemma 31 and Corollary 32, there is a non-degenerate LRS lying in the MSTV class defined by

$$u_n = \sum_{i=1}^{R} P_i(n)\lambda_i^n = \sum_{i=1}^{R}\sum_{j=0}^{\deg P_i} c_{i,j} n^j \lambda_i^n$$

such that if $M^n\boldsymbol{x} \in S$ then $u_n = 0$, and furthermore $h(\lambda_i), h(c_{i,j}) = \mathsf{poly}(\|(M,\boldsymbol{x},S)\|)$, $\deg(\lambda_i) \leq d$ and $c_{i,j} \in \mathbb{Q}(\lambda_1,\ldots,\lambda_R)$ for all i,j. Moreover, u arises as a linear combination of $d-t$ linearly independent LRS such that u has minimal support, meaning that $R \leq t+1$. Therefore, letting $\mathbb{K} = \mathbb{Q}(\lambda_1,\ldots,\lambda_R)$, we have $D = [\mathbb{K} : \mathbb{Q}] \leq d^{t+1}$. Finally, Theorem 33 implies that if $u_n = 0$, then $n < 2^{\mathsf{poly}(d^t, \|(M,\boldsymbol{x},S)\|)}$. ◄

Now we may prove our main complexity result. Before stating it, recall that **EqSLP** is the complete class for the problem of checking whether a polynomial-size circuit evaluates to zero. It is known that **EqSLP** $\subseteq$ **coRP** [34, 2].

► **Theorem 35.** *For every fixed constant $T \in \mathbb{N}$, when restricting to $t \leq T$, we have that $\textsc{Orbit}_{\mathbb{Q}}(d,t)$ for all (d,t) such that $t \leq 2\log_3 d$ is in $\mathbf{NP}^{\mathbf{EqSLP}} \subseteq \mathbf{NP}^{\mathbf{RP}}$. Furthermore, for every fixed constant $D \in \mathbb{N}$, when restricting to $d \leq D$, the problem is in* **coRP**.

Proof. Let $M \in \mathbb{Q}^{d\times d}$, $\boldsymbol{x} \in \mathbb{Q}^d$, and target subspace $S \subseteq \mathbb{Q}^d$ with $\dim S = t$ be given. Since we assume $t \leq T$ for fixed $T \in \mathbb{N}$, we have $d^t = \mathsf{poly}(d) = \mathsf{poly}(\|M\|)$. By Corollary 34, there is an upper bound

$$N = 2^{\mathsf{poly}(d^t, \|(M,\boldsymbol{x},S)\|)} = 2^{\mathsf{poly}(\|(M,\boldsymbol{x},S)\|)}$$

such that if $M^n\boldsymbol{x} \in S$, then $n \leq N$. Also, one may compute a basis $\boldsymbol{w}^{(1)},\ldots,\boldsymbol{w}^{(d-t)}$ of $S^\perp$ in polynomial time. Let $u^{(i)} = (\boldsymbol{w}^{(i)})^\top M^n\boldsymbol{x}$. We present an algorithm which then puts $\textsc{Orbit}_{\mathbb{Q}}(d,t)$ in $\mathbf{NP}^{\mathbf{RP}}$:

1. Guess an index $0 \leq n \leq N$;
2. Check whether $u_n^{(i)} = 0$ for all $1 \leq i \leq d-t$ as follows: build a polynomial-size circuit to compute $(\boldsymbol{w}^{(i)})^\top M^n\boldsymbol{x}$ for each $1 \leq i \leq d-t$, by using repeated squaring on M.

Now suppose that d is bounded. Since $N = 2^{\mathsf{poly}(\|(M,\boldsymbol{x},S)\|)}$, we have $\|N\| = \mathsf{poly}(\|(M,\boldsymbol{x},S)\|)$. Therefore, $\textsc{Orbit}_{\mathbb{Q}}(d,t)$ reduces to the Bounded Skolem Problem (as defined in [7]) with input LRS $u_n = (u_n^{(1)})^2 + \cdots + (u_n^{(d-t)})^2$ and integer N. It is shown in [7] that when the order of the input LRS is bounded, the Bounded Skolem Problem lies in **coRP**. Since the order of u is bounded by a function in d, we thus have that the $\textsc{Orbit}_{\mathbb{Q}}(d,t)$ with bounded ambient dimension d is in **coRP**. ◄

References

1 S. Akshay, Nikhil Balaji, Aniket Murhekar, Rohith Varma, and Nikhil Vyas. Near-Optimal Complexity Bounds for Fragments of the Skolem Problem. In Christophe Paul and Markus Bläser, editors, *37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)*, volume 154 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 37:1–37:18, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.STACS.2020.37`.

2 Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. *SIAM Journal on Computing*, 38(5):1987–2006, 2009. `doi:10.1137/070697926`.

3 Shaull Almagor, Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. Deciding ω-regular properties on linear recurrence sequences. *Proc. ACM Program. Lang.*, 5(POPL), January 2021. `doi:10.1145/3434329`.

4 Shaull Almagor, Joël Ouaknine, and James Worrell. The Semialgebraic Orbit Problem. In Rolf Niedermeier and Christophe Paul, editors, *36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019)*, volume 126 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.STACS.2019.6`.

5 Piotr Bacik. Completing the Picture for the Skolem Problem on Order-4 Linear Recurrence Sequences. *TheoretiCS*, 4, 2025. `doi:10.46298/theoretics.25.28`.

6 Piotr Bacik, Joël Ouaknine, David Purser, and James Worrell. On the p-adic Skolem Problem, April 2025. arXiv:2504.14413. `doi:10.48550/arXiv.2504.14413`.

7 Piotr Bacik, Joël Ouaknine, and James Worrell. On the Complexity of the Skolem Problem at Low Orders. In *Proceedings of the 2026 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 5255–5269, 2026. `doi:10.1137/1.9781611978971.191`.

8 Piotr Bacik and Anton Varonka. On the Subspace Orbit Problem and the Simultaneous Skolem Problem, 2026. `doi:10.48550/arXiv.2601.18349`.

9 Christel Baier, Florian Funke, Simon Jantsch, Toghrul Karimov, Engel Lefaucheux, Florian Luca, Joël Ouaknine, David Purser, Markus A. Whiteland, and James Worrell. The Orbit Problem for Parametric Linear Dynamical Systems. In Serge Haddad and Daniele Varacca, editors, *32nd International Conference on Concurrency Theory (CONCUR 2021)*, volume 203 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 28:1–28:17, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.CONCUR.2021.28`.

10 Yuri Bilu. Skolem Problem for Linear Recurrence Sequences with 4 Dominant Roots (after Mignotte, Shorey, Tijdeman, Vereshchagin and Bacik), March 2025. arXiv:2501.16290. `doi:10.48550/arXiv.2501.16290`.

11 Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. Skolem Meets Schanuel. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.MFCS.2022.20`.

12 E. Bombieri and J. Vaaler. On Siegel's Lemma. *Inventiones mathematicae*, 73:11–32, 1983. URL: `http://eudml.org/doc/143033`.

13 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, pages 941–950, New York, NY, USA, 2013. Association for Computing Machinery. `doi:10.1145/2488608.2488728`.

14 Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the Complexity of the Orbit Problem. *J. ACM*, 63(3):23:1–23:18, 2016. `doi:10.1145/2857050`.

15 Ventsislav Chonev, Joël Ouaknine, and James Worrell. The Polyhedron-Hitting Problem. *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms*, 2015:940–956, July 2015. doi:10.1137/1.9781611973730.64.

16 Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, Sadegh Soudjani, and James Worrell. The Pseudo-Skolem Problem is Decidable. In Filippo Bonchi and Simon J. Puglisi, editors, *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, volume 202 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 34:1–34:21, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2021.34.

17 Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, and James Worrell. The Pseudo-Reachability Problem for Diagonalisable Linear Dynamical Systems. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, pages 40:1–40:13, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2022.40.

18 Michael A. Harrison. *Lectures on Linear Sequential Machines.* Academic Press, Inc., USA, 1969.

19 R. Kannan and R. J. Lipton. Polynomial-Time Algorithm for the Orbit Problem. *J. ACM*, 33(4):808–821, August 1986. doi:10.1145/6490.6496.

20 Ravindran Kannan and Richard J. Lipton. The orbit problem is decidable. In *Proceedings of the twelfth annual ACM symposium on Theory of computing - STOC '80*, pages 252–261, Los Angeles, California, United States, 1980. ACM Press. doi:10.1145/800141.804673.

21 Toghrul Karimov. *Algorithmic verification of linear dynamical systems.* PhD thesis, Saarländische Universitäts- und Landesbibliothek, 2023. doi:10.22028/D291-41630.

22 Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. *What's Decidable About Discrete Linear Dynamical Systems?*, pages 21–38. Springer Nature Switzerland, Cham, 2022. doi:10.1007/978-3-031-22337-2_2.

23 Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. Multiple reachability in linear dynamical systems. In *2025 40th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 651–663, 2025. doi:10.1109/LICS65433.2025.00055.

24 Toghrul Karimov, Engel Lefaucheux, Joël Ouaknine, David Purser, Anton Varonka, Markus A. Whiteland, and James Worrell. What's decidable about linear loops? *Proc. ACM Program. Lang.*, 6(POPL), January 2022. doi:10.1145/3498727.

25 Toghrul Karimov, Joël Ouaknine, and James Worrell. On LTL Model Checking for Low-Dimensional Discrete Linear Dynamical Systems. In Javier Esparza and Daniel Kráľ, editors, *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 54:1–54:14, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2020.54.

26 A.N. Krylov. On the numerical solution of the equation which determines the frequencies of small vibrations of material systems for technical questions (in russian). *Bulletin of the Academy of Sciences of the USSR*, pages 491–539, 1931.

27 Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2(5):417–421, August 1953. doi:10.1007/BF02590997.

28 Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. On the skolem problem and the skolem conjecture. In *Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '22, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3531130.3533328.

29 Kurt Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38:50–60, 1935.

30 Carl D. Meyer. *Matrix analysis and applied linear algebra.* Number 189 in Other titles in applied mathematics. Siam, Society for Industrial and Applied Mathematics, Philadelphia, PA, second edition edition, 2023.

31 M. Mignotte and M. Waldschmidt. On algebraic numbers of small height: Linear forms in one logarithm. *Journal of Number Theory*, 47(1):43–62, 1994. doi:10.1006/jnth.1994.1025.

32 Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999. doi:10.1007/978-3-662-03983-0.

33 Joël Ouaknine and James Worrell. On linear recurrence sequences and loop termination. *ACM SIGLOG News*, 2(2):4–13, 2015. doi:10.1145/2766189.2766191.

34 Arnold Schönhage. On the power of random access machines. In Hermann A. Maurer, editor, *Automata, Languages and Programming*, pages 520–529, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg. doi:10.1007/3-540-09510-1_42.

35 Thoralf Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. 8. Skand. Mat.-Kongr., 163-188 (1935)., 1935.

36 R. Tijdeman, M. Mignotte, and T.N. Shorey. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik*, 349:63–76, 1984. URL: http://eudml.org/doc/152622.

37 Lloyd N. Trefethen and David Bau. *Numerical Linear Algebra*. SIAM, Philadelphia, PA, 1997.

38 N.K. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical notes of the Academy of Sciences of the USSR*, 38:609–615, 1985. URL: https://link.springer.com/article/10.1007/BF01156238.

39 Michel Waldschmidt. *Diophantine Approximation on Linear Algebraic Groups*, volume 326 of *Grundlehren der mathematischen Wissenschaften*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000. doi:10.1007/978-3-662-11569-5.