The Orbit Problem in Higher Dimensions [*]

Ventsislav Chonev
Dept. of Computer Science
Oxford University
chonev@cs.ox.ac.uk

Joël Ouaknine
Dept. of Computer Science
Oxford University
joel@cs.ox.ac.uk

James Worrell
Dept. of Computer Science
Oxford University
jbw@cs.ox.ac.uk

ABSTRACT

We consider higher-dimensional versions of Kannan and Lipton's Orbit Problem—determining whether a target vector space V may be reached from a starting point x under repeated applications of a linear transformation A. Answering two questions posed by Kannan and Lipton in the 1980s, we show that when V has dimension one, this problem is solvable in polynomial time, and when V has dimension two or three, the problem is in $\mathbf{NP}^{\mathbf{RP}}$.

Categories and Subject Descriptors

F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems—*Number-theoretic computations*; F.4.3 [**Formal Languages**]: Decision problems

General Terms

Algorithms, Theory, Verification

Keywords

Matrix powers, Orbit Problem, Skolem's Problem

1. INTRODUCTION

The *Orbit Problem* was introduced by Harrison in [17] as a formulation of the reachability problem for linear sequential machines. The problem is stated as follows:

> Given a square matrix $A \in \mathbb{Q}^{m \times m}$ and vectors $x, y \in \mathbb{Q}^m$, decide whether there exists a non-negative integer n such that $A^n x = y$.

The decidability of this problem remained open for over ten years, until it was shown to be decidable in polynomial time by Kannan and Lipton [19]. In the conclusion of the journal version of their work [20], Kannan and Lipton discuss a higher-dimensional extension of the Orbit Problem, as follows:

> Given a square matrix $A \in \mathbb{Q}^{m \times m}$, a vector $x \in \mathbb{Q}^m$, and a subspace V of $\mathbb{Q}^m$, decide whether there exists a non-negative integer n such that $A^n x \in V$.

As Kannan and Lipton point out, the higher-dimensional Orbit Problem is closely related to the *Skolem Problem*: given a square matrix $A \in \mathbb{Q}^{m \times m}$ and vectors $x, y \in \mathbb{Q}^m$, decide whether there exists a non-negative integer n such that $y^T A^n x = 0$. Indeed, the Skolem Problem is the special case of the higher-dimensional Orbit Problem in which the target space V has dimension $m - 1$. The sequence of numbers $u_n = y^T A^n x$ is a linear recurrence sequence. A well-known result, the Skolem-Mahler-Lech theorem, states that the set of zeros of any linear recurrence union of a finite set and finitely many arithmetic progressions [16, 21, 22, 28]. Moreover, it is known how to effectively compute the arithmetic progressions [5]. The main difficulty in deciding Skolem's Problem is to determine whether the finite component of the set of zeros is empty.

The decidability of the Skolem Problem has been open for many decades [14], and it is therefore unsurprising that there has been virtually no progress on the higher-dimensional Orbit Problem since its introduction in [20]. In fact, decidability of the Skolem Problem for matrices of dimension three and four [24, 33] only came in the two years prior to the publication of [20], and there has been no substantial progress on this front since. In terms of lower bounds, the strongest known result for the Skolem Problem is $\mathbf{NP}$-hardness [7], which therefore carries over to the unrestricted version of the higher-dimensional Orbit Problem.

Kannan and Lipton speculated in [20] that for target spaces of dimension one the Orbit Problem might be solvable, "hopefully with a polynomial-time bound". They moreover observed that the cases in which the target space V has dimension two or three seem "harder", and proposed this line of research as an approach towards the Skolem Problem. In spite of this, to the best of our knowledge, no progress has been recorded on the higher-order Orbit Problem in the intervening two-and-a-half decades.

Our main results are the following. We show that the higher-dimensional Orbit Problem can be solved in polynomial time if the target space V has dimension one, and in $\mathbf{NP}^{\mathbf{RP}}$ if the target space has dimension two or three. While we make extensive use of the work of [24, 33] on Skolem's

[*] This research was supported by the EPSRC.

STOC'13, June 1-4, 2013, Palo Alto, California, USA.

Problem, our results, in contrast, are independent of the dimension of the matrix A.

The following example illustrates some of the phenomena that emerge in the Orbit Problem for two-dimensional target spaces. Consider the following matrix and initial vector:

$$A = \begin{bmatrix} 4 & 6 & 14 & 21 \\ -8 & -2 & -28 & -7 \\ -2 & -3 & -6 & -9 \\ 4 & 1 & 12 & 3 \end{bmatrix} \qquad x = \begin{bmatrix} 28 \\ -14 \\ -10 \\ 5 \end{bmatrix}$$

Then with target space

$$V = \{(u_1, u_2, u_3, u_4) \in \mathbb{Q}^4 : 4u_1 + 7u_3 = 0,\, 4u_2 + 7u_4 = 0\}$$

it can be shown that $A^n x \in V$ if and only if n has residue 2 modulo 6. Such periodic behaviour can be analysed in terms of the eigenvalues of the matrix A. These are $\lambda\omega$, $\overline{\lambda}\omega$, $\lambda\overline{\omega}$, and $\overline{\lambda\omega}$, where $\omega = e^{\pi i/3}$ is a primitive 6-th root of unity and $\lambda = (-1 + i\sqrt{39})/2$. The key observation is that the eigenvalues of A fall into only two classes under the equivalence relation $\sim$, defined by $\alpha \sim \beta$ if and only if α/β is a root of unity.

We will show that for a two-dimensional target space V, for any matrix A whose eigenvalues have at least three classes under $\sim$, there is at most one exponent n such that $A^n x \in V$. Computable bounds on such an n can be obtained utilising the above-mentioned work of [24, 33] on Skolem's Problem, which in turn is based on results in transcendental number theory. Unfortunately the resulting bounds on n are exponential in the size of the problem representation, leading to an $\mathbf{NP}^{\mathbf{RP}}$ *guess-and-check* procedure, in which an **RP** oracle is used to check whether $A^n x \in V$ for a guessed value of n. Finally, the case in which the eigenvalues of A have at most two equivalence classes under $\sim$ can be handled using techniques akin to those used in the solution of the original Orbit Problem.

1.1 Related Work

Aside from its connection to the Skolem Problem, the higher-dimensional Orbit Problem is closely related to termination problems for linear programs (see, e.g., [4, 31, 8]) and to reachability questions for discrete linear dynamical systems (cf. [14]). Another related problem is the *chamber hitting problem*, which replaces the target space with an intersection of half-spaces. In [29], the chamber hitting problem is related to decision problems in formal language theory. Let us also mention the more recent work of Arvind and Vijayaraghavan [2] which places the original Orbit Problem in the logspace counting hierarchy **GapLH**.

Another generalisation or the Orbit Problem is the so-called $A\ B\ C$ problem. This asks, given commuting rational matrices A, B and C, whether there exist integers i and j such that $A^i B^j = C$. This problem was shown to be decidable in polynomial time in [34]. A continuous version of the Orbit Problem is considered in [13]. Here one studies linear differential equations of the form $x'(t) = Ax(t)$ for a rational matrix A. The problem is to decide, for a given initial condition $x(0)$ and target vector v, whether there exists t such that $x(t) = v$. The main result of [13] shows decidability of this problem.

In the present paper, we provide full proofs of the main results for the cases in which the dimension of the target space V is one or two. Proof details for the case in which V has dimension three have been consigned to the full version of this paper [11].

The structure of the paper is as follows. Section 2 gathers together mathematical background on algebraic numbers. In Section 3 we reduce the fixed-dimension Orbit Problem to the fixed-dimension matrix power problem. In Section 4, we prove that the one-dimensional version is decidable in polynomial time. In Section 5 we show decidability for the two-dimensional case. Finally, section 6 concludes the paper with the discussion of the complexity of the two-dimensional case.

2. PRELIMINARIES

2.1 Algebraic Numbers

In this section we briefly summarise results about algebraic-number computation that will be used in the paper. Fuller explanations of the notions below can be found in [12].

A complex number α is *algebraic* if it is a root of a polynomial with rational coefficients. The *minimal polynomial* of α, denoted f_α, is the unique monic polynomial of least degree which vanishes at α. If f_α has integer coefficients then we say that α is an *algebraic integer.* The *degree* of α is defined to be the degree of f_α, and the *height* of α is defined to be the maximum absolute value of the coefficients of the integer polynomial cf_α, where c is the least common multiple of the denominators of the coefficients of f_α. The roots of f_α (including α itself) are called the *Galois conjugates* of α. For each Galois conjugate β of α there is a monomorphism $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$ with $\sigma(\alpha) = \beta$, where $\mathbb{Q}(\alpha)$ is the field obtained by adjoining α to $\mathbb{Q}$.

The *norm* of α, denoted $\mathcal{N}(\alpha)$, is the product of its Galois conjugates. Observe that $\mathcal{N}(\alpha)$ is equal in absolute value to the constant term in the minimal polynomial f_α.

A standard representation of an algebraic number α comprises its minimal polynomial f_α, along with a rational approximation of $Re(\alpha)$ and $Im(\alpha)$ of sufficient precision to distinguish α from its Galois conjugates. More precisely, we represent α by the tuple

$$(f_\alpha, p, q, R) \in (\mathbb{Q}[x] \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}) ,$$

meaning that α is the unique root of f_α inside the circle in the complex plane of radius R centred at $p+iq$. A separation bound due to Mignotte [23] states that for roots $\alpha_i \neq \alpha_j$ of a polynomial $f(x)$,

$$|\alpha_i - \alpha_j| > \frac{\sqrt{6}}{n^{(n+1)/2} H^{n-1}} \qquad (1)$$

where n and H are the degree and height of f, respectively. Thus, if R is restricted to be less than a quarter of the root separation bound, the representation is well-defined. Given a univariate polynomial f, it is known how to obtain standard representations for each of its roots in polynomial time [26]. Moreover, though the representation of a given algebraic number is not unique, we can check whether two representations denote the same number in polynomial time.

Henceforth, when we say an algebraic number α is given, we will assume we have a standard representation of α. We will denote by $\|\alpha\|$ the length of this representation, assuming that integers are expressed in binary and rationals are expressed as pairs of integers. Thus for a rational a, $\|a\|$ is just the sum of the lengths of its numerator and denominator written in binary. Overloading notation, for a polynomial $p \in \mathbb{Q}[x]$, $\|p\|$ will denote $\sum_{i=0}^{n} \|p_i\|$ where n is the degree of the polynomial and p_i are its coefficients.

The root-separation bound (1) implies that $|\alpha|$ and $1/(1-|\alpha|)$ are at most exponentially large in $\|\alpha\|$. This yields a polynomial upper bound for $\log|\alpha|$ and an exponential upper bound for $1/\log|\alpha|$ in terms of $\|\alpha\|$.

Lemma 1. *Given standard representations of algebraic numbers α, β and a polynomial $p \in \mathbb{Q}[x]$, it is possible to compute standard representations of $\alpha \pm \beta$, $\alpha\beta^{\pm 1}$ and $p(\alpha)$ in time polynomial in the length of the input (that is, in $\|\alpha\| + \|\beta\| + \|p\|$).*

Given standard representations it is trivial to check whether $\alpha = \beta$ and whether α belongs to one of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.

A *number field* $\mathbb{K}$ is a finite-dimensional extension of $\mathbb{Q}$. The set of algebraic integers in $\mathbb{K}$ forms a ring, denoted $\mathcal{O}$. Given $\alpha \in \mathcal{O}$, (α) denotes the principal ideal generated by α. Given two ideals I, J in $\mathcal{O}$, the product IJ is the ideal generated by the elements ab, where $a \in I$ and $b \in J$. An ideal P of $\mathcal{O}$ is *prime* if $ab \in P$ implies $a \in P$ or $b \in P$. The *fundamental theorem of ideal theory* states that any non-zero ideal in $\mathcal{O}$ can be written as the product of prime ideals, and the representation is unique if the order of the prime ideals is ignored.

With a prime ideal P we associate a *valuation* $v_P : \mathcal{O} \setminus \{0\} \to \mathbb{N}$ as follows:

$$v_P(\alpha) = k \text{ if and only if } P^k \mid (\alpha) \text{ and } P^{k+1} \nmid (\alpha)$$

That is, $v_P(\alpha)$ is the number of times P appears in the factorisation into prime ideals of the principal ideal (α). We also define $v_P(0) = \infty$.

The function v_P satisfies the following properties:

- $v_P(\alpha\beta) = v_P(\alpha) + v_P(\beta)$
- $v_P(\alpha + \beta) \geq \min\{v_P(\alpha), v_P(\beta)\}$
- If $v_P(\alpha) \neq v_P(\beta)$, then $v_P(\alpha+\beta) = \min\{v_P(\alpha), v_P(\beta)\}$

Recall that for any $\alpha \in \mathbb{K} \setminus \mathcal{O}$ we can find $\beta \in \mathcal{O}$ and $n \in \mathbb{Z}$ such that $\alpha = \beta/n$. We extend v_P to $\mathbb{K}$ by defining $v_P(\alpha) = v_P(\beta) - v_P(n)$. The first of the three properties of v_P above guarantees that this value is independent of the choice of β and n, making the extension of v_P to $\mathbb{K}$ well-defined. Note that the extension preserves the above three properties of v_P. Note also that if α is not an algebraic integer then in the equation $\alpha = \beta/n$, above, β and n cannot be associates, and thus $v_P(\alpha) \neq 0$ for some prime ideal P.

We can bound the valuation of an algebraic number in terms of its norm as follows:

$$v_P(\alpha) \leq \log_2 |\mathcal{N}(\alpha)|\,.$$

It follows that $v_P(\alpha)$ is at most polynomial in the length of the representation of α.

2.2 Algebraic-Number Power Problems

One of the main techniques used in [20] to study the zero-dimensional Orbit Problem is to reduce the analysis of powers of a rational matrix to that of powers of an algebraic number. In particular [20] showed that, given algebraic numbers α and β, one can determine in polynomial time whether $\alpha^n = \beta$ for some integer n. We recall this result and some associated ideas below. We also state some lower bounds on $\alpha^n - \beta$ in case $\alpha^n \neq \beta$. These are used in the generalisation of the Orbit Problem to higher dimensions, following Mignotte's and Vereshchagin's partial decidability results on Skolem's Problem [24, 33].

We first consider the problem of deciding whether $\alpha^n = 1$ for some n, that is, whether α is a root of unity. Recall that the minimal polynomial of a primitive r-th root of unity is the r-th *cyclotomic polynomial*, which has degree $\varphi(r)$, where φ is Euler's totient function. From the (crude) lower bound $\varphi(r) \geq \sqrt{r/2}$ one obtains:

Proposition 2. *[20] If α has degree d and is a primitive r-th root of unity, then $r \leq 2d^2$.*

Generalising to the case of deciding whether $\alpha^n = \beta$ for some n, we have the following result.

Theorem 3. *[20] There exists a polynomial P such that for any algebraic numbers α and β, where α is not a root of unity, if $\alpha^n = \beta$ for a natural number n, then n is at most $P(||\alpha||, ||\beta||)$.*

The main idea underlying the proof of Theorem 3 is a result of Blanksby and Montgomery [6] stating that if α is an algebraic integer of degree d that is not a root of unity then α has a Galois conjugate $\sigma(\alpha)$ such that

$$|\sigma(\alpha)| > 1 + \frac{1}{30d^2\log(6d)} \tag{2}$$

We use this result in similar fashion to generalise Theorem 3 as follows:

Theorem 4. *There exists a polynomial P such that for any algebraic numbers α, a and b, where α is not a root of unity, if $\alpha^n = an + b$ then n is at most $P(||\alpha||, ||a||, ||b||)$.*

Proof. Let d denote the degree of α. First, if α is an algebraic integer, then by Blanksby and Montgomery's theorem, it has a Galois conjugate $\sigma(\alpha)$ such that

$$|\sigma(\alpha)| > 1 + \frac{1}{30d^2\log(6d)} \tag{3}$$

Now $|\sigma(an + b)|$ grows linearly in n, whereas $|\sigma(\alpha^n)|$ grows exponentially in n, with the base of the exponent having lower bound (3). We thus obtain a polynomial bound on n.

Second, suppose α is not an algebraic integer. Then there exists a prime ideal P in the ring of integers of $\mathbb{Q}(\alpha, a, b)$ such that $v_P(\alpha) \neq 0$. Then we have

$$\begin{aligned} |v_P(\alpha^n)| &= n|v_P(\alpha)| \\ &= |v_P(a + bn)| \\ &\leq \log_2 |\mathcal{N}(a + bn)|\,. \end{aligned} \tag{4}$$

But, from discussion of norms in Section 2, the value

$$\log_2 |\mathcal{N}(a + bn)|$$

is polynomial in $\log_2 n$ and the size of the representations of α, a, and b. Since the left-hand side of (4) grows linearly in n, and the right-hand side grows polynomially in $\log_2 n$, we obtain a polynomial bound on n such that the equation can hold. □

We pass now from the problem of deciding whether $\alpha^n = \beta$ for some n, to the question of lower bounds on $|\alpha^n - \beta|$ in case this quantity is non-zero. We consider lower bounds with respect to the usual Archimedean absolute value as well as with respect to P-adic valuations.

The Archimedean lower bound depends on the following theorem of Baker and Wüstholz [3] on linear forms of logarithms of algebraic numbers. Throughout, log refers to the principal value of the complex logarithm given by $\log z = \log|z| + i \arg z$, where $-\pi < \arg z \leq \pi$.

Theorem 5. *(Baker and Wüstholz [3]) Let $\alpha_1, \ldots, \alpha_m$ be algebraic numbers other than 0 or 1, and let $b_1, \ldots, b_m$ be rational integers. Write*

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_m \log \alpha_m \,.$$

Let $A_1, \ldots, A_m, B \geq e$ be real numbers such that, for each $j \in \{1, \ldots, m\}$, A_j is an upper bound for the height of α_j, and B is an upper bound for $|b_j|$. Let d be the degree of the extension field $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ over $\mathbb{Q}$. If $\Lambda \neq 0$, then

$$\log|\Lambda| > -(16md)^{2(m+2)} \log(A_1) \ldots \log(A_m) \log(B) \,.$$

We will need the following special case of Theorem 5, which is standard.

Corollary 6. *Let α and β be algebraic numbers of height at most $H \geq 4$ such that $\mathbb{Q}(\alpha, \beta)$ has degree at most d. If $\alpha\beta^n \neq 1$ then*

$$|1 - \alpha\beta^n| > \frac{1}{2} \, n^{-(48d)^{10} \log^2(H)} \,.$$

Proof. From the power series expansion $\log(1 + w) = \sum_{n=1}^{\infty} (-1)^{n-1} w^n/n$ we get that $|\log(1+w)| \leq 2|w|$ for $|w| \leq 1/2$. Writing $w = \alpha\beta^n - 1$, we have

$$2|1 - \alpha\beta^n| \geq |\log(\alpha\beta^n)| = |n \log \beta + \log \alpha + 2k\pi i| \qquad (5)$$

for some $k \in \mathbb{Z}$ with $|k| \leq n$. Observing that $\log(-1) = i\pi$, the result follows by applying Theorem 5 to the right-hand side of (5). □

The next theorem, a special case of a result due to van der Poorten [32], is an analogous bound for P-adic valuations.

Theorem 7. *(van der Poorten [32]) Let α, β be algebraic numbers of degree at most d belonging to a number field $\mathbb{K}$ and with heights at most H. Let P be a prime ideal of $\mathbb{K}$ containing the rational prime p. Then for any integer $n \geq 8$ such that $\alpha\beta^n \neq 1$ we have*

$$v_P(\alpha\beta^n - 1) \leq (48d)^{36} \, \frac{p^d}{\log(p)} \, (\log(H) \log(n))^2 \,.$$

3. REDUCTION

3.1 Matrix Power Problem

Let A be a rational $m \times m$ matrix, $x \in \mathbb{Q}^m$ a vector, and V a vector space specified by a basis $y_1, \ldots, y_k \in \mathbb{Q}^m$. We wish to decide whether there exists $n \in \mathbb{N}$ such that $A^n x \in V$. In our technical development we work with $\mathbb{C}$ as field of scalars, regarding x as an element of $\mathbb{C}^n$ and consider V as a subspace of $\mathbb{C}^n$. Since all input data are rational this does not affect the problem.

Recall (e.g., from [15, Section 58]) that we can decompose $\mathbb{Q}^m$ as the direct sum of two subspaces U_1 and U_2 that are both invariant under A, such that A is nilpotent on U_1 and invertible on U_2. Using this decomposition, which can be computed in polynomial time, we can assume without loss of generality that the matrix A in the Orbit Problem is invertible.

Next, following [19], we reformulate the generalized Orbit Problem as a version of the so-called *matrix power problem*.

Let ν be maximal such that $x, Ax, \ldots, A^\nu x$ are linearly independent, and write P for the matrix whose columns are $x, Ax, \ldots, A^\nu x$. Notice that the column space of P is an invariant subspace for A. Indeed we have $A^{\nu+1}x = q_0 x + q_1 Ax + \ldots + q_\nu A^\nu x$ for some $q_0, \ldots, q_\nu \in \mathbb{Q}$, so that $AP = PM$, where

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & q_0 \\ 1 & 0 & \cdots & 0 & q_1 \\ 0 & 1 & \cdots & 0 & q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & q_\nu \end{bmatrix}$$

Writing $e = (1, 0, \ldots, 0)^T$, we have $Pe = x$. Furthermore, let $W = \{y : Py \in V\}$ be the pre-image of V under P. Then

$$\begin{aligned} A^n x \in V \quad &\Leftrightarrow \quad A^n Pe \in V \\ &\Leftrightarrow \quad PM^n e \in V \\ &\Leftrightarrow \quad M^n e \in W \,. \end{aligned}$$

Let $w_1, \ldots, w_t$ be a basis of W. Then for $a_1, \ldots, a_t \in \mathbb{C}$,

$$\begin{aligned} & M^n e = \textstyle\sum_{i=1}^t a_i w_i \\ \Leftrightarrow \quad & M^n [e \; Me \; \ldots \; M^\nu e] = \textstyle\sum_{i=1}^t a_i [w_i \; Mw_i \; \ldots \; M^\nu w_i] \\ \Leftrightarrow \quad & M^n = \textstyle\sum_{i=1}^t a_i T_i \,, \end{aligned}$$

where $T_i = [w_i \; Mw_i \; \ldots \; M^\nu w_i]$. Thus $A^n x \in V$ if and only if $M^n \in \mathcal{T}$, where $\mathcal{T} = \mathrm{span}\{T_1, \ldots, T_t\}$. Note also that $\dim(\mathcal{T}) = \dim(W) \leq \dim(V)$.

Thus we have reduced the Orbit Problem to the problem of determining whether some power of a given matrix lies in a given vector space of matrices. Notice that the reduction does not increase the dimension of the target space.

We perform one further reduction step. It is clear that within the target space $\mathcal{T}$ it suffices to consider only matrices of the shape $p(M)$, where p is a polynomial with rational coefficients. Writing $\mathcal{T}' = \mathcal{T} \cap \mathrm{span}\{p(M) \mid p \in \mathbb{Q}[x]\}$, we have $M^n \in \mathcal{T} \iff M^n \in \mathcal{T}'$. Clearly also $\dim(\mathcal{T}') \leq \dim(\mathcal{T})$.

In summary, we have reduced the Orbit Problem to the *matrix power problem*: given a rational matrix $M \in \mathbb{Q}^{m \times m}$ and polynomials $p_1, \ldots, p_s \in \mathbb{Q}[x]$, determine whether M^n lies in the span of $p_1(M), \ldots, p_s(M)$ for some n. All operations described in the reduction can be performed in polynomial time using standard techniques from linear algebra. Finally, we remark that the matrix M produced by the reduction is non-singular since A was assumed to be non-singular.

3.2 The Master System

Suppose now that we have an instance $(A, p_1, \ldots, p_s)$ of the matrix power problem, where A is an $m \times m$ matrix. A natural approach would be to write $A = P^{-1}JP$ for some similarity transformation P and Jordan matrix J. However, the procedure for computing P, P^{-1}, and J from A in polynomial time is sophisticated [10]. The difficulty is that the splitting field of the minimal polynomial of A may have degree exponential in m. Instead, similarly to [20], we pursue a self-contained approach that allows us to separately consider each root of the minimal polynomial of A.

We begin by calculating the minimal polynomial f_A of A and obtaining standard representations of its roots $\alpha_1, \ldots, \alpha_k$ (which are the eigenvalues of A). This may be done in polynomial time, see Section 2. We denote by $mul(\alpha_i)$ the multiplicity of an eigenvalue α_i as a root of f_A. Clearly $mul(\alpha_i) \le m$.

Fix an exponent $n \ge m$ and coefficients $a_1, \ldots, a_s \in \mathbb{C}$, and define the polynomials $P(x) = \sum_{i=1}^{s} a_i p_i(x)$ and $Q(x) = x^n$. Denote by $P^{(j)}$ the j-th derivative of P. It is easy to see that $P(A) = Q(A)$ if and only if

$$P^{(j)}(\alpha_i) = Q^{(j)}(\alpha_i) \quad \text{for } 1 \le i \le k,\ 0 \le j < mul(\alpha_i) \tag{6}$$

Indeed, $P - Q$ is zero at A if and only if f_A divides $P - Q$, that is, each α_i is a root of $P - Q$ with multiplicity at least $mul(\alpha_i)$. This is equivalent to saying that each α_i is a root the first $mul(\alpha_i) - 1$ derivatives of $P - Q$.

Thus in order to decide whether there exists an exponent n and coefficients a_i such that $A^n = \sum_{i=1}^{s} a_i p_i(A)$, it is sufficient to solve a system of equations (6) in which the unknowns are $n \in \mathbb{N}$ and $a_1, \ldots, a_s \in \mathbb{C}$. Each eigenvalue α_i contributes $mul(\alpha_i)$ equations which specify that P and its first $mul(\alpha_i) - 1$ derivatives all vanish at α_i.

We refer to (6) as the *Master System.* We denote by $eq(\alpha_i, j)$ the j-th derivative equation $P^{(j)}(\alpha_i) = Q^{(j)}(\alpha_i)$ contributed to the master system by α_i. For example, if f_A has roots α_1, α_2, α_3 with respective multiplicities $1, 1, 2$, and the target space is spanned by $p_1(A)$ and $p_2(A)$, then the Master System contains four equations:

$$\begin{array}{rcl} \alpha_1^n & = & a_1 p_1(\alpha_1) + a_2 p_2(\alpha_1) \\ \alpha_2^n & = & a_1 p_1(\alpha_2) + a_2 p_2(\alpha_2) \\ \alpha_3^n & = & a_1 p_1(\alpha_3) + a_2 p_2(\alpha_3) \\ n\alpha_3^{n-1} & = & a_1 p_1'(\alpha_3) + a_2 p_2'(\alpha_3) \end{array}$$

4. ONE-DIMENSIONAL VERSION

In this section we prove the following result.

Theorem 8. *The one-dimensional Orbit Problem is decidable in polynomial time.*

Applying the reduction to the matrix power problem from Section 3.1, assume that we are given an instance of the one-dimensional matrix power problem (A, p), with A a non-singular rational matrix and $p \in \mathbb{Q}[x]$. We wish to decide in polynomial time whether $A^n \in \text{span}\{p(A)\}$ for some n. We assume without loss of generality that n is at least the dimension of A; smaller witnesses n can be found by brute force. Under this assumption we have constructed an equivalent Master System of equations (6) in the exponent $n \in \mathbb{N}$ and the coefficient $a \in \mathbb{C}$. For example, if the roots of f_A are $\alpha_1, \alpha_2, \alpha_3$ with multiplicities $1, 2, 1$, the system is:

$$\begin{array}{rcl} \alpha_1^n & = & ap(\alpha_1) \\ \alpha_2^n & = & ap(\alpha_2) \\ n\alpha_2^{n-1} & = & ap'(\alpha_2) \\ \alpha_3^n & = & ap(\alpha_3) \end{array}$$

In this section we will describe how such systems can be solved in polynomial time.

Since A is non-singular, the eigenvalues α_i are all non-zero and thus the left-hand side of each equation $eq(\alpha_i, j)$ is non-zero. We can check in polynomial time whether any equation $eq(\alpha_i, j)$ has a right-hand side that is zero for $a \neq 0$. If so, the system is unsatisfiable. Otherwise, we assume that the right-hand side of each equation $eq(\alpha_i, j)$ is non-zero. In particular, we freely divide one equation by another.

Next we compute standard representations of all quotients α_i/α_j. By Proposition 2 we can decide in polynomial time whether each quotient is a root of unity. We now consider three cases.

Case 1. Some quotient α_i/α_j is not a root of unity. Dividing equation $eq(\alpha_i, 0)$ by $eq(\alpha_j, 0)$ yields

$$\left(\frac{\alpha_i}{\alpha_j}\right)^n = \frac{p(\alpha_i)}{p(\alpha_j)} \tag{7}$$

By Lemma 1 in Section 2, we can compute standard representations of $p(\alpha_i)/p(\alpha_j)$ and α_i/α_j in polynomial time. Then by Theorem 3, n is bounded by a polynomial in the input. Thus it suffices to check whether $A^n \in \text{span}\{p(A)\}$ for all n up to the bound.

Case 2. All quotients α_i/α_j are roots of unity, and all roots of f_A are simple. For given n, any single equation $\alpha_i^n = ap(\alpha_i)$ has a solution $a \in \mathbb{C}$. Thus the Master System is equivalent to the system of equations of the form (7) obtained by dividing $eq(\alpha_i, 0)$ by $eq(\alpha_j, 0)$ for all $i < j$, as shown in (7).

Suppose α_i/α_j is an r-th root of unity. If the right-hand side of (7) is also an r-th root of unity, then the solutions of (7) are $n \equiv t \bmod r$ for some t. If not, then (7) has no solution, so the entire Master System (6) has no solution, and the problem instance is negative. By Lemma 1, we can determine in polynomial time whether the right-hand side of (7) is a root of unity, and if so, calculate t. We transform each equation in (7) into an equivalent congruence in n. This gives a system of congruences in n which is equivalent to the set of quotient equations (7). Thus the problem instance is positive iff the system of congruences has a solution. We then solve the congruences using the Chinese Remainder Theorem.

Case 3. All quotients α_i/α_j are roots of unity, and f_A has repeated roots. As in Case 2 we can obtain a system of equations that is equisatisfiable with the Master System by considering quotients of every pair of equations in the latter. In fact, by transitivity, there is no need to consider quotients of every pair of equations. For each $i < j$, we divide $eq(\alpha_i, 0)$ by $eq(\alpha_j, 0)$, obtaining (7). Furthermore, for each repeated root α_i of f_A and multiplicity $0 \le j < mul(\alpha_i) - 1$, we divide $eq(\alpha_i, j)$ by $eq(\alpha_i, j+1)$, obtaining

$$\frac{\alpha_i}{n - j} = \frac{p^{(j)}(\alpha_i)}{p^{(j+1)}(\alpha_i)}$$

which is equivalent to

$$n = j + \frac{p^{(j+1)}(\alpha_i)}{p^{(j)}(\alpha_i)} \alpha_i\,. \tag{8}$$

Recall from Case 2 that each equation of the form (7) is equivalent to a congruence on n that can be computed in polynomial time. For each equation of the form (8) we calculate the right-hand side and check whether it is in $\mathbb{N}$. If not, then the system has no solution. Otherwise, (8) points to a single candidate n. We do this for all such equations. If they point to the same value of n, and this value of n satisfies all the congruences derived from equations of the form (7), then the Master System has a solution. Otherwise the Master System has no solution.

5. TWO-DIMENSIONAL VERSION

Suppose we are given an instance I of the two-dimensional Orbit Problem, comprising an $m \times m$ rational matrix A and rational vectors $x, y_1, y_2 \in \mathbb{Q}^m$. Denote by $||I||$ the size of the instance. The question is to determine whether there exists $n \in \mathbb{N}$ such that $A^n x \in \text{span}\{y_1, y_2\}$. Our main result is as follows:

THEOREM 9. *The two-dimensional Orbit Problem is decidable in* $\mathbf{NP}^{\mathbf{RP}}$.

In fact we will show that the two-dimensional Orbit Problem is decidable in $\mathbf{NP}^{\mathbf{EqSLP}}$. Recall that **EqSLP** is the problem of determining whether an arithmetic circuit, with addition, multiplication and subtraction gates, evaluates to zero. Since this problem is known to be in **coRP** [27], we obtain the desired bound for the Orbit Problem.

The decidability of this problem, as well as the complexity bound, relies on showing that if $A^n x \in \text{span}\{y_1, y_2\}$ for some n, then it already holds for some exponent $n \in 2^{||I||^{O(1)}}$. Given this, there is a straightforward $\mathbf{NP}^{\mathbf{EqSLP}}$ decision procedure: (i) guess the exponent n; (ii) compute $A^n x$ as an arithmetic circuit in polynomial time by iterated squaring; (iii) check that the $m \times 3$ matrix $B = [A^n x \; y_1 \; y_2]$ has rank at most 2 with a single call to an **EqSLP** oracle. For the last step, recall that $\ker(B) = \ker(B^T B)$, and so B has rank at most 2 if and only if $B^T B$ is singular. This last condition can be determined by checking zeroness of the 3×3 determinant $\det(B^T B)$.

Our first step is to apply the reduction from Section 3.1, obtaining an instance of the matrix power problem (A, p, q), with A non-singular. We wish to decide whether there exists $n \in \mathbb{N}$ such that $A^n \in \mathit{span}\,\{p(A), q(A)\}$. We assume that n is at least the dimension of A: smaller witnesses n can be found by brute force. Under this assumption we have constructed in Section 3.2 an equivalent *Master System* of equations in variables $n \in \mathbb{N}$ and $u, v \in \mathbb{C}$, of the form

$$\alpha_i^n = up^{(j)}(\alpha_i) + vq^{(j)}(\alpha_i) \tag{9}$$

for α_i a root of the minimal polynomial f_A of A and $0 \leq j < \mathit{mul}(\alpha_i)$.

In solving (9) we can assume that $u, v \neq 0$, otherwise we revert to the one-dimensional case. Also, since A is non-singular, each eigenvalue α_i is non-zero, and it suffices to search for solutions of (9) in which the right-hand side is non-zero.

Define an equivalence relation $\sim$ on the roots of the minimal polynomial f_A by

$$\alpha \sim \beta \text{ if and only if } \alpha/\beta \text{ is a root of unity}.$$

The proof proceeds by a case analysis on the number of equivalence classes.

Case I: At least three equivalence classes

Pick eigenvalues α, β, γ in different equivalence classes. Then the Master System contains the following three equations:

$$\begin{aligned} \alpha^n &= up(\alpha) + vq(\alpha) \\ \beta^n &= up(\beta) + vq(\beta) \\ \gamma^n &= up(\gamma) + vq(\gamma) \end{aligned}$$

Eliminating u and v from the above equations, we can compute algebraic numbers a, b, c such that

$$a\alpha^n + b\beta^n + c\gamma^n = 0\,. \tag{10}$$

The decidability proof of the Skolem Problem for recurrences of order 3 [24, 33] shows that there are computable bounds on n such that expressions of the form (10) hold. We recall the argument from [24] below, quantifying these bounds in order to justify the complexity claim in Theorem 9.

Assume that a, b, c are all non-zero. The case in which only one of a, b or c is zero can be handled by Theorem 3. Dividing by $a\alpha^n$, (10) is equivalent to

$$1 + \frac{b}{a}\left(\frac{\beta}{\alpha}\right)^n + \frac{c}{a}\left(\frac{\gamma}{\alpha}\right)^n = 0\,. \tag{11}$$

We now consider two sub-cases. The first sub-case is that α/γ is an algebraic integer of degree d. Since α/γ is not a root of unity, by Blanksby and Montgomery's theorem [6] it has a Galois conjugate $\sigma(\alpha/\gamma)$ such that

$$|\sigma(\alpha/\gamma)| > 1 + \frac{1}{30d^2 \log(6d)}\,.$$

Replacing α, β, γ with their images under the monomorphism σ we may thus assume that

$$\left|\frac{c}{a}\left(\frac{\gamma}{\alpha}\right)^n\right| < \left|\frac{c}{a}\left(1 - \frac{1}{c_1}\right)^n\right| \tag{12}$$

for some constant $c_1 = ||I||^{O(1)}$. On the other hand, applying Corollary 6, we also have

$$\left|1 + \frac{b}{a}\left(\frac{\beta}{\alpha}\right)^n\right| \geq (n/2)^{-c_2} \tag{13}$$

for a constant $c_2 = ||I||^{O(1)}$. Comparing the exponentially decaying term in (12) with the polynomially decaying term in (13), we can derive a computable bound $c_3 = ||I||^{O(1)}$ such that (10) cannot hold for $n > c_3$.

The second sub-case is that α/γ is not an algebraic integer. In particular, α/γ is not a unit, so there exists a prime ideal P such that $v_P(\gamma) \neq v_P(\alpha)$. By interchanging α and γ, if necessary, we can assume that $v_P(\gamma) > v_P(\alpha)$. Then

$$v_P\left(\frac{c}{a}\left(\frac{\gamma}{\alpha}\right)^n\right) \geq v_P(c) - v_P(a) + n\,. \tag{14}$$

On the other hand, applying Theorem 7 to the number field $\mathbb{Q}(\alpha, \beta, \gamma)$, we get

$$v_P\left(1 + \frac{b}{a}\left(\frac{\beta}{\alpha}\right)^n\right) \leq c_4(\log n)^{c_5}\,. \tag{15}$$

with $c_4 = 2^{||I||^{O(1)}}$ and $c_5 = ||I||^{O(1)}$. Combining the inequalities (14) and (15), we derive a computable bound $c_6 = 2^{||I||^{O(1)}}$ such that (10) cannot hold for $n > c_6$. Note that the exponential dependence of c_6 on $||I||$ can be traced to the term p^d in Theorem 7. Here we have $p \mid \mathcal{N}(P)$ and $\mathcal{N}(P) \mid \mathcal{N}(\gamma/\alpha)$, so that $p = 2^{||I||^{O(1)}}$.

In summary, we have a computable bound for n in $2^{||I||^{O(1)}}$ beyond which (10) cannot hold.

Case II: Two equivalence classes

First, suppose that there are roots $\alpha \not\sim \beta$, with α a repeated root of f_A. Then the Master System contains the following three equations:

$$\begin{aligned} \alpha^n &= up(\alpha) + vq(\alpha) \\ n\alpha^{n-1} &= up'(\alpha) + vq'(\alpha) \\ \beta^n &= up(\beta) + vq(\beta)\,. \end{aligned}$$

Eliminating u and v, we can compute algebraic numbers a, b, c, at least two of which are non-zero, such that

$$(a + bn)\alpha^n + c\beta^n = 0\,. \tag{16}$$

But then Theorem 4 gives a bound on n in (16) that is polynomial in $||I||$.

Now assume that all roots are simple. We will show that if the Master System is satisfiable then it has a solution in which the exponent n is bounded by an exponential function in $||I||$.

Let the two equivalence classes of roots be $\{\alpha_1, \ldots, \alpha_s\}$ and $\{\beta_1, \ldots, \beta_t\}$. Write L for the least common multiple of the orders of the roots of unity among the quotients α_i/α_j and β_i/β_j. We consider solutions of the Master System by case analysis on the value of n modulo L, so let this value be fixed. We now analyse the quotients of each pair of equations $eq(\alpha_i, 0)$ and $eq(\alpha_j, 0)$, for $1 \leq i < j \leq s$, the quotients of each pair of equations $eq(\beta_i, 0)$ and $eq(\beta_j, 0)$, for $1 \leq i < j \leq t$, as well as the quotient of $eq(\alpha_1, 0)$ by $eq(\beta_1, 0)$. It is not difficult to see that the resulting system of 'quotient equations' is equisatisfiable with the Master System.

Dividing $eq(\alpha_i, 0)$ by $eq(\alpha_j, 0)$, we have

$$\begin{aligned} \left(\frac{\alpha_i}{\alpha_j}\right)^n &= \frac{up(\alpha_i) + vq(\alpha_i)}{up(\alpha_j) + vq(\alpha_j)} \\ &= \frac{p(\alpha_i) + tq(\alpha_i)}{p(\alpha_j) + tq(\alpha_j)} \end{aligned} \tag{17}$$

where $t = v/u$. (Recall that $u \neq 0$ by assumption.) The value of the left-hand side of (17) is determined by the residue of n modulo L, which is assumed fixed. If $q(\alpha_i)p(\alpha_j) = p(\alpha_i)q(\alpha_j)$ then the right-hand side of (17) is independent of the value of t, and the equation is either satisfied for all values of t or no values of t. On the other hand, if $q(\alpha_i)p(\alpha_j) \neq p(\alpha_i)q(\alpha_j)$, then (17) is satisfied for a single value

$$t = \frac{p(\alpha_i) - p(\alpha_j)(\alpha_i/\alpha_j)^n}{q(\alpha_j)(\alpha_i/\alpha_j)^n - q(\alpha_i)} \tag{18}$$

which is determined by the residue of n modulo L.

Consider the quotient of each pair of equations $eq(\alpha_i, 0)$ and $eq(\alpha_j, 0)$, and the quotient of each pair of equations $eq(\beta_i, 0)$ and $eq(\beta_j, 0)$. For a given residue of n modulo L, this system of quotient equations is either satisfied for all values of t, no values of t, or a single value of t of the form (18).

It remains to divide $eq(\alpha_1, 0)$ by $eq(\beta_1, 0)$, yielding

$$\left(\frac{\alpha_1}{\beta_1}\right)^n = \frac{p(\alpha_1) + tq(\alpha_1)}{p(\beta_1) + tq(\beta_1)}\,. \tag{19}$$

If $q(\alpha_1)p(\beta_1) = p(\alpha_1)q(\beta_1)$ then the right-hand side of (19) is independent of t and the equation has at most one solution in n, which, if it exists, is polynomial in $||I||$ by Theorem 3. Otherwise, if $q(\alpha_1)p(\beta_1) \neq p(\alpha_1)q(\beta_1)$, then (19) has a unique solution in t for each value of n. If there is no other constraint on the value of t then we can solve (19), yielding satisfiability of the Master System for some value of n less than L. If there is a constraint on t of the form (18), then the right-hand side of (19) is bound to a single algebraic number whose representation has size polynomial in $||I||$. Then Theorem 3 yields a bound on n that is polynomial in $||I||$.

In all cases we obtain a bound on n that is exponential in $||I||$ in case the Master System is satisfiable.

Case III: One equivalence class

Let the roots be $\alpha_1, \ldots, \alpha_s$, and write L for the least common multiple of the orders of the roots of unity α_i/α_j, $i < j$. Let us consider solutions of the Master System for some fixed residue of n modulo L.

Dividing $eq(\alpha_i, j)$ by $eq(\alpha_i, j+1)$ for $0 \leq j < mul(\alpha_i) - 1$, we get that

$$\begin{aligned} \frac{\alpha_i}{n-j} &= \frac{up^{(j)}(\alpha_i) + vq^{(j)}(\alpha_i)}{up^{(j+1)}(\alpha_i) + vq^{(j+1)}(\alpha_i)} \\ &= \frac{p^{(j)}(\alpha_i) + tq^{(j)}(\alpha_i)}{p^{(j+1)}(\alpha_i) + tq^{(j+1)}(\alpha_i)} \end{aligned} \tag{20}$$

where, again, $t = v/u$.

If $q^{(j)}(\alpha_i)p^{(j+1)}(\alpha_i) = p^{(j)}(\alpha_i)q^{(j+1)}(\alpha_i)$, then the right-hand side of (20) is independent of t, and (20) has a single solution in n, whose magnitude is exponential in $||I||$. On the other hand, if $q^{(j)}(\alpha_i)p^{(j+1)}(\alpha_i) \neq p^{(j)}(\alpha_i)q^{(j+1)}(\alpha_i)$, then (20) is equivalent to a constraint of the form

$$t = \frac{an + b}{cn + d} \tag{21}$$

for algebraic numbers a, b, c and d whose representations have size polynomial in $||I||$. Note that two constraints of the form (21) yield a polynomial equation on n that is either trivial or that has two solutions in n, both at most exponential in $||I||$.

Recall that the system of equations that arises by taking the quotient of each pair $eq(\alpha_i, 0)$ and $eq(\alpha_j, 0)$ is either unsatisfiable, is satisfied for a single value of t (of the form (18)), or has solutions for all t. Considering also the constraints on t arising from quotients of the form (20), these constraints either fix n to a value that is exponential in $||I||$, or place no restriction on n. In the last case the solvability of the Master System depends only on the residue of n modulo L, so that if the system is satisfiable then it is satisfied for some $n < L$.

6. CONCLUSION

We have shown that the higher-dimensional Orbit Problem is decidable in polynomial time when the target space V has dimension one. We have also shown membership in $\mathbf{NP}^{\mathbf{EqSLP}}$ in the case $\dim(V) = 2$. The paper [11] shows the same complexity bound also holds if $\dim(V) = 3$. The proof uses similar principles, but is more complicated. It is known [27] that $\mathbf{EqSLP} \subseteq \mathbf{coRP}$, so membership in $\mathbf{NP}^{\mathbf{RP}}$ follows immediately.

Decidability of the higher-dimensional Orbit Problem in the case $\dim(V) = 4$ would immediately yield decidability of Skolem's Problem for five-dimensional matrices. The latter is currently open: a decidability proof was claimed in [14] but, as pointed out in [25], the argument seems to have a serious gap.

A careful analysis of Cases II and III of the two-dimensional Orbit Problem reveals that there is a polynomial-time procedure to handle these cases. The idea is to use the Chinese Remainder Theorem, as in the one-dimension problem. In fact, the failure to obtain a polynomial-time algorithm in the two-dimensional problem can be traced to a single factor: the dependence of the P-adic lower bound in Theorem 7 on the prime p (whose magnitude can be exponential in the problem instance). Tijdeman [30] has remarked that the dependence of the bound in Theorem 7 on p is an impediment for some applications. Bugeaud [9] shows that this dependence can be avoided in certain restricted circumstances, which unfortunately do not appear to hold in the case at hand.

We have previously remarked that the higher-dimensional Orbit Problem is **NP**-hard in general. However the hardness proof [7], via Skolem's Problem, requires that the dimension of the target space V be unbounded. On the other hand, achieving a polynomial upper bound in case the target V has dimension two would seem to require either an improvement in the Diophantine approximation bound in Theorem 7 or a different approach to the problem.

Roughly speaking, the **EqSLP** oracle used by our main decision procedure is invoked to check equality of entries of the matrix A^n, where the exponent is given in binary. In general the complexity of **EqSLP**, which is equivalent to polynomial identity testing, is a major open problem, cf. [1]. However it may be possible to make progress on the special case of matrix exponentiation; see [18] for some initial results in this direction.

7. REFERENCES

[1] E. Allender, P. Bürgisser, J. Kjeldgaard-Pedersen, and P. B. Miltersen. On the complexity of numerical analysis. *SIAM J. Comput.*, 38(5):1987–2006, 2009.

[2] V. Arvind and T. Vijayaraghavan. The orbit problem is in the GapL hierarchy. *J. Comb. Optim.*, 21(1):124–137, 2011.

[3] A. Baker and G. Wüstholz. Logarithmic forms and group varieties. *Jour. Reine Angew. Math.*, 442:19–62, 1993.

[4] A. M. Ben-Amram, S. Genaim, and A. N. Masud. On the termination of integer loops. *ACM Trans. Program. Lang. Syst.*, 34(4):16, 2012.

[5] J. Berstel and M. Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France*, 104, 1976.

[6] P. Blanksby and H. Montgomery. Algebraic integers near the unit circle. *Acta Arith.*, pages 355–369, 1971.

[7] V. Blondel and N. Portier. The presence of a zero in an integer linear recurrent sequence is NP-hard to decide. *Linear Algebra and Its Applications*, 2002.

[8] M. Braverman. Termination of integer linear programs. In *CAV*, volume 4144 of *Lecture Notes in Computer Science*, pages 372–385. Springer, 2006.

[9] Y. Bugeaud. Linear forms in p-adic logarithms and the diophantine equation $(x^n - 1)/(x - 1) = y^q$. *Math. Proc. Cambridge Phil. Soc.*, 127:373–381, 1999.

[10] J.-Y. Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. *Int. J. Found. Comput. Sci.*, 5(3/4):293–302, 1994.

[11] V. Chonev, J. Ouaknine, and J. Worrell. The Orbit Problem in higher dimensions (long version). *CoRR*, arXiv:1303.2981, 2013.

[12] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 1993.

[13] E. Hainry. Reachability in linear dynamical systems. In *CiE*, volume 5028 of *Lecture Notes in Computer Science*, pages 241–250. Springer, 2008.

[14] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem's problem – on the border between decidability and undecidability. *TUCS Technical Report*, (683), 2005.

[15] P. Halmos. *Finite-Dimensional Vector Spaces.* Springer, 1974.

[16] G. Hansel. Une démonstration simple du théorème de Skolem-Mahler-Lech. *Theoretical Computer Science*, 43:91 – 98, 1986.

[17] M. Harrison. *Lectures on sequential machines.* Academic Press, Orlando, 1969.

[18] M. Hirvensalo, J. Karhumäki, and A. Rabinovich. Computing partial information out of intractable: Powers of algebraic numbers as an example. *Journal of Number Theory*, 130:232–253, 2010.

[19] R. Kannan and R. J. Lipton. The orbit problem is decidable. In *Proceedings of the twelfth annual ACM symposium on Theory of computing*, STOC '80, pages 252–261, New York, NY, USA, 1980. ACM.

[20] R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *J. ACM*, 33(4):808–821, 1986.

[21] C. Lech. A note on recurring series. *Arkiv för Matematik*, 2:417–421, 1953.

[22] K. Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38:51–60, 1935.

[23] M. Mignotte. Some useful bounds. *Computer Algebra*, pages 259–263, 1982.

[24] M. Mignotte, T. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *Jour. Reine Angew. Math.*, 349:63 – 76, 1984.

[25] J. Ouaknine and J. Worrell. Decision problems for linear recurrence sequences. In *RP*, volume 7550 of *Lecture Notes in Computer Science*, pages 21–28, 2012.

[26] V. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12):97 – 138, 1996.

[27] A. Schönhage. On the power of random access machines. In H. Maurer, editor, *Automata, Languages and Programming*, volume 71 of *Lecture Notes in Computer Science*, pages 520–529. Springer, 1979.

[28] T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. *Skand. Mat. Kongr.*, 8:163–188, 1934.

[29] S. P. Tarasov and M. N. Vyalyi. Orbits of linear maps and regular languages. *CoRR*, arXiv:1011.1842, 2010.

[30] R. Tijdeman. Some applications of diophantine approximation. *Number Theory for the Millennium III*, pages 261–284, 2002.

[31] A. Tiwari. Termination of linear programs. In *CAV*, volume 3114 of *Lecture Notes in Computer Science*, pages 70–82. Springer, 2004.

[32] A. J. van der Poorten. Linear forms in logarithms in

the p-adic case. *Transcendence Theory: Advances and Applications*, pages 29–57, 1977.

[33] N. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical Notes*, 38:609–615, 1985.

[34] J.-Yi Cai, R. J. Lipton, and Y. Zalcstein. The complexity of the A B C problem. *SIAM J. Comput.*, 29(6):1878–1888, 2000.