Information Processing Letters 115 (2015) 11–14

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Continuous-time orbit problems are decidable in polynomial-time

Taolue Chen [a,*], Nengkun Yu [c,d], Tingting Han [b]

[a] Department of Computer Science, Middlesex University London, United Kingdom
[b] Department of Computer Science and Information Systems, Birkbeck, University of London, United Kingdom
[c] Institute for Quantum Computing, University of Waterloo, Canada
[d] Department of Mathematics & Statistics, University of Guelph, Canada

ARTICLE INFO

Article history:
Received 7 March 2014
Received in revised form 10 August 2014
Accepted 10 August 2014
Available online 22 August 2014
Communicated by M. Yamashita

Keywords:
Dynamical systems
Differential equation
Computational complexity
Continuous-time orbit problem
Linear algebra

ABSTRACT

We place the continuous-time orbit problem in P, sharpening the decidability result shown by Hainry [7].

1. Introduction

In this paper, we study the *linear dynamical system* whose dynamics is described by a *linear differential equation*. Formally, given a matrix $A \in \mathbb{K}^{n\times n}$ and a vector $\vec{\zeta} \in \mathbb{K}^n$, the *trajectory* of the system, $\vec{x}(t)$ for $t \in \mathbb{R}_{\geq 0}$, is defined as the solution of the following Cauchy problem:

$$\begin{cases} \frac{d\vec{x}}{dt} = A\vec{x} \\ \vec{x}(0) = \vec{\zeta}. \end{cases} \tag{1}$$

Here $\mathbb{K}$ is an arbitrary field and $\mathbb{R}$ is the real field.

Linear dynamical systems have found applications in a wide range of scientific areas, for instance, theoretical biology, economics, and quantum computing. One of the basic algorithmic questions regarding a linear dynamical system is the *orbit problem*, which can be formulated as follows: Given the trajectory $\vec{x}(t)$ determined by $A \in \mathbb{K}^{n\times n}$ and $\vec{\zeta} \in \mathbb{K}^n$, and a point $\vec{\xi} \in \mathbb{K}^n$, decide whether there exists some time $t \in \mathbb{R}_{\geq 0}$ such that $\vec{x}(t) = \vec{\xi}$. Namely, whether $\vec{\xi}$ can be reached from $\vec{\zeta}$.

The decidability of the orbit problem has been shown by Hainry [7], when $\mathbb{K}$ is the rational field. In this note we improve this result by showing that it is in P. Our algorithm follows Hainry [7] in general, i.e., by Jordan norm forms and results from transcendental number theory such as the Gelfond–Schneider theorem and the Lindemann–Weierstrass theorem. However, our arguments are considerably simpler. In particular, it turns out that the distinction of two Jordan norm forms based on eigenvalues of A in [7] is unnecessary, neither is the use trigonometric functions. These simplifications enable us to perform a complexity analysis which appeared to be hard and was lacking by Hainry's arguments.

Related work. Ref. [8] studied the discrete-time orbit problem and showed that the problem is in P. The upper-bound was improved to the logspace counting hierarchy (together with a $\mathsf{C}_{=\mathsf{L}}$ lower-bound) [1]. The techniques employed

* Corresponding author.

http://dx.doi.org/10.1016/j.ipl.2014.08.004
0020-0190/

there are considerably different from the current paper. Ref. [5] considered a generalisation of the orbit problem, i.e. the orbit problem in higher dimensions, and related the problem to the celebrated Skolem problem. The authors showed that this problem is in P when the dimension is one, and is in $\mathsf{NP}^{\mathsf{RP}}$ for dimension two or three. Ref. [3] studied the continuous-time Skolem problem. The authors identified decidability for this problem in some special cases, and showed that the related nonnegativity problem is NP-hard in general (whereas the decidability is left open).

2. Preliminaries

Throughout the paper, we write $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{A}$, and $\mathbb{R}$ for the set of complex, rational, algebraic, and real numbers, respectively. For any complex number $z = a + bi$ where $a, b \in \mathbb{R}$ and i is the imaginary unit, we denote the real part and the imaginary part of z by $\Re(z) = a$ and $\Im(z) = b$ respectively.

Definition 1. An *algebraic number* is a number that is a root of a non-zero polynomial in one variable with rational coefficients. An algebraic number α is represented by $(P, (a, b), \rho)$ where P is the *minimal polynomial* of α, $a+bi$ is an approximation of α such that $|\alpha - (a + bi)| < \rho$ and α is the only root of P in the open ball $\mathcal{B}(a + bi, \rho)$.

It is well known that a root of a non-zero polynomial in one variable with coefficients of algebraic numbers is also algebraic. Moreover, given the representations of two algebraic numbers α and β, the representations of $\alpha \pm \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$ can be computed in polynomial time, so is the equality checking [6].

In the sequel, we list some basic facts from transcendental number theory [2].

Theorem 1 *(Gelfond–Schneider). Assume $a, b \in \mathbb{A}$ with $a \neq 0, 1$ and $b \notin \mathbb{Q}$, then any value of a^b is a transcendental number.*

Corollary 1. *Assume $a, b \in \mathbb{A}$ with $\ln(a), \ln(b)$ being linearly independent over $\mathbb{Q}$, then they are linearly independent over $\mathbb{A}$.*

Theorem 2 *(Lindemann–Weierstrass). If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers which are linearly independent over the rational numbers $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$.*

Corollary 2. *For any $\alpha \neq 0$, one of α and e^α must be transcendental.*

Definition 2. A *Jordan block* is a square matrix of the following form

$$\begin{bmatrix} \lambda & & & \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{bmatrix}$$

A square matrix J is in *Jordan norm form* if

$$J = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_k \end{bmatrix}$$

where each J_i for $1 \le i \le k$ is a Jordan block.

The following proposition is a basic fact of linear algebra.

Proposition 1. *Any matrix $A \in \mathbb{Q}^{n\times n}$ is similar to a matrix in Jordan form. Namely, there exist some $P \in \mathbb{A}^{n\times n}$ and $J \in \mathbb{A}^{n\times n}$ in Jordan form such that $A = P^{-1}JP$.*

For any matrix $A \in \mathbb{C}^{n\times n}$, the *exponential* of A, denoted by e^A, is the $n \times n$ matrix given by

$$e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k.$$

For the differential equation (1), the solution can be written as

$$\vec{x}(t) = e^{tA}\vec{\zeta},$$

and evidently the orbit problem is to determine whether there exists $t \in \mathbb{R}_{\ge 0}$ such that $e^{tA}\vec{\zeta} = \vec{\xi}$.

3. Main results

In this section we fix an instance of the orbit problem, i.e., $A \in \mathbb{Q}^{n\times n}$ and $\vec{\zeta}, \vec{\xi} \in \mathbb{Q}^n$. We consider the Jordan norm form of A such that $A = P^{-1}JP$, where $P \in \mathbb{A}^{n\times n}$ and $J \in \mathbb{A}^{n\times n}$, i.e.,

$$J = \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_k \end{bmatrix}$$

Moreover, we denote the eigenvalues for the Jordan blocks by $\lambda_1, \cdots, \lambda_k$, and we write

$$\vec{x} = P\vec{\zeta} = \begin{bmatrix} \vec{x}_1 \\ \vdots \\ \vec{x}_k \end{bmatrix} \quad \text{and} \quad \vec{y} = P\vec{\xi} = \begin{bmatrix} \vec{y}_1 \\ \vdots \\ \vec{y}_k \end{bmatrix}$$

such that for each $1 \le i \le k$, $\vec{x}_i$ or $\vec{y}_i$ is of the size of J_i. For simplicity, we group the eigenvalue λ_i and the corresponding vectors $\vec{x}_i$ and $\vec{y}_i$ together and refer to *block* B_i. We say $B_i = (\lambda_i, \vec{x}_i, \vec{y}_i)$ is *oblivious* if $\vec{x}_i = \mathbf{0}$; otherwise, it is *non-oblivious*.

Theorem 3. *To determine whether there exists $t \in \mathbb{R}_{\ge 0}$ such that $e^{tA}\vec{\zeta} = \vec{\xi}$ for $A \in \mathbb{Q}^{n\times n}$ and $\vec{\zeta}, \vec{\xi} \in \mathbb{Q}^n$ is in P.*

Proof. Observe that

$$e^{tA} = e^{tP^{-1}JP} = P^{-1}e^{tJ}P,$$

and thus

$$e^{tA}\vec{\zeta} = \vec{\xi} \quad \text{iff} \quad e^{tJ}(P\vec{\zeta}) = P\vec{\xi}.$$

Namely, $e^{tJ}\vec{x} = \vec{y}$, and thus for each $1 \le i \le k$ we have

$$e^{tJ_i}\vec{x}_i = \vec{y}_i.$$

In the case that B_i is oblivious (i.e., $\vec{x}_i = \mathbf{0}$), it must be the case that $\vec{y}_i = \mathbf{0}$. In the sequel, we shall focus on the non-oblivious blocks.

Observe that

$$e^{tJ_i} = e^{t\lambda_i}\begin{bmatrix} 1 & & & & \\ t & 1 & & & \\ \frac{t^2}{2} & t & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \\ \frac{t^s}{s!} & \cdots & \frac{t^2}{2} & t & 1 \end{bmatrix},$$

where s is the size of J_i. We consider the following two cases.

(i) $\lambda_i = 0$. Then it must be the case that

$$\begin{bmatrix} 1 & & & & \\ t & 1 & & & \\ \frac{t^2}{2} & t & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \\ \frac{t^s}{s!} & \cdots & \frac{t^2}{2} & t & 1 \end{bmatrix}\vec{x}_i = \vec{y}_i.$$

Recall that entries of $\vec{x}_i$ and $\vec{y}_i$ are all algebraic numbers. Hence, as we assume that $\vec{x}_i \neq \mathbf{0}$, we have that $t \in \mathbb{A}$.

(ii) $\lambda_i \neq 0$. Then

$$e^{t\lambda_i}\begin{bmatrix} 1 & & & & \\ t & 1 & & & \\ \frac{t^2}{2} & t & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \\ \frac{t^s}{s!} & \cdots & \frac{t^2}{2} & t & 1 \end{bmatrix}\vec{x}_i = \vec{y}_i.$$

Recall that $\vec{x}_i \neq \mathbf{0}$. Clearly $e^{\lambda_i t} \in \mathbb{A}$. Note that Corollary 2 asserts that either $e^{\lambda_i t} \notin \mathbb{A}$ or $\lambda_i t \notin \mathbb{A}$. Hence $\lambda_i t \notin \mathbb{A}$ and thus $t \notin \mathbb{A}$. Furthermore, we claim that the size of the Jordan block (i.e., s) must be 1, because otherwise clearly $t \in \mathbb{A}$ which is a contradiction.

We distinguish the following two cases:

(a) All non-oblivious blocks are of eigenvalue 0. By case (i), $t \in \mathbb{A}$. Choose one of such blocks, we have an equation of the form

$$\begin{bmatrix} 1 & & & & \\ t & 1 & & & \\ \frac{t^2}{2} & t & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \\ \frac{t^s}{s!} & \cdots & \frac{t^2}{2} & t & 1 \end{bmatrix}\vec{u} = \vec{v}$$

and $\vec{u} \neq \mathbf{0}$. Let $i^* = \min\{i \mid \vec{u}_i \neq 0\}$ (such i^* must exist). Hence it must be the case that $t = \frac{\vec{v}_{i^*}}{\vec{u}_{i^*}}$.

(b) There exists at least one non-oblivious block whose eigenvalue is nonzero. Then by case (ii), $t \notin \mathbb{A}$. It follows that all non-oblivious blocks must have nonzero eigenvalues and all such Jordan blocks are of size 1. That is, without loss of generality we have an equation of the form

$$\begin{bmatrix} e^{t\lambda_1} & & & \\ & e^{t\lambda_2} & & \\ & & \ddots & \\ & & & e^{t\lambda_\ell} \end{bmatrix}\begin{bmatrix} u_1 \\ \vdots \\ u_\ell \end{bmatrix} = \begin{bmatrix} v_1 \\ \vdots \\ v_\ell \end{bmatrix} \qquad (2)$$

such that for each $1 \le i \le \ell$, $u_i \neq 0$ and $\lambda_i \neq 0$. Here ℓ is the number of non-oblivious blocks. Writing $z_i = \frac{v_i}{u_i}$, we have that, for $1 \le i \le \ell$,

$$e^{\lambda_i t} = z_i.$$

We then claim that Eq. (2) has a solution $t \in \mathbb{R}_{\ge 0}$ iff

1. for any $1 \le i, j \le \ell$, $\frac{\lambda_i}{\lambda_j} \in \mathbb{Q}$ and $z_i^{\lambda_i} = z_j^{\lambda_j}$; and
2. there exist λ_i and z_i such that
   (2a) Either $\Re(z_i) > 0$, $\Im(\lambda_i) = 0$, and $\Im(z_i) = 0$;
   (2b) or $\Re(\lambda_i) = 0$ and $|z_i| = 1$.

The "if" part is obvious. To see the "only if" part, firstly it is easy to see that for $1 \le i, j \le \ell$, $z_i^{\lambda_j} = z_j^{\lambda_i}$. Namely, $\lambda_j \ln(z_i) - \lambda_i \ln(z_j) = 0$. By Corollary 1, $\ln(z_i)$ and $\ln(z_j)$ are linear independent over $\mathbb{Q}$. Hence $\frac{\lambda_i}{\lambda_j} = \frac{\ln(z_i)}{\ln(z_j)} \in \mathbb{Q}$.

Now let's focus on any $e^{\lambda_i t} = z_i$. Assume that $\lambda = a + bi$ and $z = c + di$, where $a, b, c, d \in \mathbb{R} \cap \mathbb{A}$. Recall that $\lambda_i \neq 0$. We consider the following cases:

– $a \neq 0$ and $b = 0$. Then t exists iff $c > 0$ and $d = 0$. This is equivalent to the case (2a).
– $a = 0$ and $b \neq 0$. Then t exists iff $c^2 + d^2 = 1$. This is equivalent to the case (2b).
– $a \neq 0$ and $b \neq 0$. It follows that

$$\begin{cases} e^{at} = \sqrt{c^2 + d^2} \in \mathbb{A} \\ e^{bti} = \frac{c+di}{\sqrt{c^2+d^2}} \in \mathbb{A} \end{cases}$$

It follows that $(\sqrt{c^2 + d^2})^{i\frac{b}{a}} = \frac{c+di}{\sqrt{c^2+d^2}}$. By Theorem 1 we must have that $i\frac{b}{a} \in \mathbb{Q}$ which is a contradiction. Hence this case is actually vacuous.

Based on the above arguments, the algorithm is rather straightforward and we can analyse its complexity. By the result of [4], there is a polynomial-time algorithm to perform the Jordan decomposition for A, namely, one can compute the λ_i's, $\vec{x}$ and $\vec{y}$ in polynomial time. Hence we can check for each oblivious block (λ_i, x_i, y_i) whether $y_i = \mathbf{0}$. If this is not the case, the algorithm is terminated and returns "No". Otherwise, we can determine either case (a) or case (b).

- In case (a), we can check whether $t = \frac{\vec{v}_{i^*}}{\vec{u}_{i^*}}$ is the solution for all non-oblivious blocks. This can be done easily in polynomial time.
- In case (b), we can check whether conditions 1 and 2 are satisfied. To check $\frac{\lambda_i}{\lambda_j} \in \mathbb{Q}$, it suffices to check whether the degree of the minimal polynomial of $\frac{\lambda_i}{\lambda_j}$ is at most 1, which can be done in polynomial time. On top of this, checking $z_i^{\lambda_i} = z_j^{\lambda_j}$ amounts to checking

$z_i^{r_{ij}} = z_j$ where $r_{ij} = \frac{\lambda_i}{\lambda_j}$, which can done in polynomial time as well. Furthermore it is trivial to check, for some λ_i and z_i whether (2a) or (2b) holds.

This completes the proof. □

4. Conclusion

In this paper, we have shown that the continuous-time orbit problem is decidable in polynomial-time. A very natural question is to consider the continuous-time orbit problem in higher dimensions. Combining the arguments of [5] and this paper, one can settle the case of dimension two or three; one can also link this problem to the continuous-time Skolem problem. However, solving this problem thoroughly seems to be difficult without a breakthrough (cf. [3]), notwithstanding some recent development for the discrete-time case [9]. It is also interesting to see whether the P upper-bound established here can be improved further, along the line of [1]. The main difficulty seems to lie in factoring polynomials which is needed for Jordan decomposition in [4]. To the best of our knowledge, the best upper-bound is P (by, e.g., the LLL algorithm) which obstructs further improvement inside P. We leave it an interesting open problem how to circumvent this difficulty.

Acknowledgement

We are grateful to the referees for their constructive comments.

References

[1] V. Arvind, T.C. Vijayaraghavan, The orbit problem is in the GapL hierarchy, in: X. Hu, J. Wang (Eds.), COCOON, in: Lect. Notes Comput. Sci., vol. 5092, Springer, 2008, pp. 160–169.
[2] A. Baker, Transcendental Number Theory, Cambridge University Press, 1990.
[3] P.C. Bell, J.-C. Delvenne, R.M. Jungers, V.D. Blondel, The continuous Skolem–Pisot problem, Theor. Comput. Sci. 411 (40–42) (2010) 3625–3634.
[4] J. Cai, Computing Jordan normal forms exactly for commuting matrices in polynomial time, Int. J. Found. Comput. Sci. 5 (3/4) (1994) 293–302.
[5] V. Chonev, J. Ouaknine, J. Worrell, The orbit problem in higher dimensions, in: D. Boneh, T. Rougarden, J. Feigenbaum (Eds.), STOC, ACM, 2013, pp. 941–950.
[6] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 1993.
[7] E. Hainry, Reachability in linear dynamical systems, in: A. Beckmann, C. Dimitracopoulos, B. Löwe (Eds.), CiE, in: Lect. Notes Comput. Sci., vol. 5028, Springer, 2008, pp. 241–250.
[8] R. Kannan, R.J. Lipton, Polynomial-time algorithm for the orbit problem, J. ACM 33 (4) (1986) 808–821.
[9] J. Ouaknine, J. Worrell, Positivity problems for low-order linear recurrence sequences, in: C. Chekuri (Ed.), SODA, SIAM, 2014, pp. 366–379.