On the Monniaux Problem in Abstract Interpretation*

Nathanaël Fijalkow[1], Engel Lefaucheux[2], Pierre Ohlmann[3], Joël Ouaknine[2,4], Amaury Pouly[5], and James Worrell[4]

[1] CNRS, LaBRI, France and The Alan Turing Institute, UK
[2] Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany
[3] IRIF, Université Paris 7, France
[4] Department of Computer Science, Oxford University, UK
[5] CNRS, IRIF, Université Paris Diderot, France

Abstract. The Monniaux Problem in abstract interpretation asks, roughly speaking, whether the following question is decidable: given a program P, a safety (*e.g.*, non-reachability) specification φ, and an abstract domain of invariants $\mathcal{D}$, does there exist an inductive invariant $\mathcal{I}$ in $\mathcal{D}$ guaranteeing that program P meets its specification φ. The Monniaux Problem is of course parameterised by the classes of programs and invariant domains that one considers.

In this paper, we show that the Monniaux Problem is undecidable for unguarded affine programs and semilinear invariants (unions of polyhedra). Moreover, we show that decidability is recovered in the important special case of simple linear loops.

1 Introduction

Invariants are one of the most fundamental and useful notions in the quantitative sciences, appearing in a wide range of contexts, from gauge theory, dynamical systems, and control theory in physics, mathematics, and engineering to program verification, static analysis, abstract interpretation, and programming language semantics (among others) in computer science. In spite of decades of scientific work and progress, automated invariant synthesis remains a topic of active research, especially in the fields of program analysis and abstract interpretation, and plays a central role in methods and tools seeking to establish correctness properties of computer programs; see, *e.g.*, [21], and particularly Sec. 8 therein.

The focus of the present paper is the ***Monniaux Problem*** on the decidability of the existence of separating invariants, which was formulated by David

* Nathanaël Fijalkow, Pierre Ohlmann, and Amaury Pouly were supported by the Agence Nationale de la Recherche through the project Codys (ANR-18-CE40-0007). Joël Ouaknine was supported by ERC grant AVS-ISS (648701) and by DFG grant 389792660 as part of TRR 248 (see https://perspicuous-computing.science). James Worrell was supported by EPSRC Fellowship EP/N008197/1.

Monniaux in [26, 27] and also raised by him in a series of personal communications with various members of the theoretical computer science community over the past five years or so. There are in fact a multitude of versions of the Monniaux Problem—indeed, it would be more appropriate to speak of a *class* of problems rather than a single question—but at a high level the formulation below is one of the most general:

> Consider a program P operating over some numerical domain (such as the integers or rationals), and assume that P has an underlying finite control-flow graph over the set of nodes $Q = \{q_1, \ldots, q_r\}$. Let us assume that P makes use of d numerical variables, and each transition $q \xrightarrow{t} q'$ comprises a function $f_t : \mathbb{R}^d \to \mathbb{R}^d$ as well as a guard $g_t \subseteq \mathbb{R}^d$. Let $x, y \in \mathbb{Q}^d$ be two points in the ambient space. By way of intuition and motivation, we are interested in the reachability problem as to whether, starting in location q_1 with variables having valuation x, it is possible to reach location q_r with variables having valuation y, by following the available transitions and under the obvious interpretation of the various functions and guards. Unfortunately, in most settings this problem is well-known to be undecidable.
>
> A collection $\{I_q \mid q \in Q\}$ is called an (inductive[6]) *invariant* if for each transition $q \xrightarrow{t} q'$, we have that $f_t(\mathcal{I}_q \cap g_t) \subseteq \mathcal{I}_{q'}$. If it additionally satisfies that $x \in \mathcal{I}_{q_1}$ and $y \notin \mathcal{I}_{q_r}$, then it is a *separating invariant* for program P. Clearly, the existence of a separating invariant constitutes a proof of non-reachability for P with the given x and y.
>
> Let $\mathcal{D} \subseteq 2^{\mathbb{R}^d}$ be an 'abstract domain' for P, *i.e.*, a collection of subsets of $\mathbb{R}^d$. For example, $\mathcal{D}$ could be the collection of all convex polyhedra in $\mathbb{R}^d$, or the collection of all closed semialgebraic sets in $\mathbb{R}^d$, etc.
>
> The Monniaux Problem can now be formulated as a decision question: is it possible to adorn each control location q with an element $\mathcal{I}_q \in \mathcal{D}$ such that the collection $\{I_q \mid q \in Q\}$ forms a separating invariant?
>
> Associated with this decision problem, in positive instances one is also potentially interested in the synthesis problem, *i.e.*, the matter of algorithmically producing a suitable separating invariant $\{\mathcal{I}_q : q \in Q\}$.

The Monniaux Problem is therefore parameterised by a number of items, key of which are (i) the abstract domain $\mathcal{D}$ under consideration, and (ii) the kind of functions and guards allowed in transitions.

Our main interest in this paper lies in the *decidability* of the existence of separating invariants for various instances of the Monniaux Problem. We give below a cursory cross-sectional survey of existing work and results in this direction.

Arguably the earliest positive result in this area is due to Karr, who showed that strongest affine invariants (conjunctions of affine equalities) for affine programs (no guards, and all transition functions are given by affine expressions)

[6] In the remainder of this paper, the term 'invariant' shall always refer to the inductive kind.

could be computed algorithmically [20]. Note that the ability to synthesise strongest (*i.e.*, smallest with respect to set inclusion) invariants immediately entails the decidability of the Monniaux Problem instance, since the existence of *some* separating invariant is clearly equivalent to whether the *strongest* invariant is separating. Müller-Olm and Seidl later extended this work on affine programs to include the computation of strongest polynomial invariants of fixed degree [28], and a randomised algorithm for discovering affine relations was proposed by Gulwani and Necula [16]. More recently, Hrushovski *et al.* showed how to compute a basis for *all* polynomial relations at every location of a given affine program [17].

The approaches described above all compute invariants consisting exclusively of conjunctions of *equality* relations. By contrast, an early and highly influential paper by Cousot and Halbwachs considers the domain of convex closed polyhedra [9], for programs having polynomial transition functions and guards. Whilst no decidability results appear in that paper, much further work was devoted to the development of restricted polyhedral domains for which theoretical guarantees could be obtained, leading (among others) to the *octagon domain* of Miné [25], the *octahedron domain* of Clarisó and Cortadella [6], and the *template polyhedra* of Sankaranarayanan *et al.* [30]. In fact, as observed by Monniaux [27], if one considers a domain of convex polyhedra having a *uniformly bounded* number of faces (therefore subsuming in particular the domains just described), then for any class of programs with polynomial transition relations and guards, the existence of separating invariants becomes decidable, as the problem can equivalently be phrased in the first-order theory of the reals.

One of the central motivating questions for the Monniaux Problem is whether one can always compute separating invariants for the full domain of polyhedra. Unfortunately, on this matter very little is known at present. In recent work, Monniaux showed undecidability for the domain of convex polyhedra and the class of programs having affine transition functions and polynomial guards [27]. One of the main results of the present paper is to show undecidability for the domain of *semilinear sets*[7] and the class of affine programs (without any guards)—in fact, affine programs with only a single control location and two transitions:

Theorem 1. *Let $A, B \in \mathbb{Q}^{d\times d}$ be two rational square matrices of dimension d, and let x, y be two points in $\mathbb{Q}^d$. Then the existence of a semilinear set $\mathcal{I} \subseteq \mathbb{R}^d$ having the following properties:*

1. *$x \in \mathcal{I}$;*
2. *$A\mathcal{I} \subseteq \mathcal{I}$ and $B\mathcal{I} \subseteq \mathcal{I}$; and*
3. *$y \notin \mathcal{I}$*

is an undecidable problem.

It is worth pointing out that the theorem remains valid even for a fixed d (our proof shows undecidability for $d = 96$, but this value could be improved).

[7] A semilinear set consists of a finite union of polyhedra, or equivalently is defined as the solution set of a Boolean combination of linear inequalities.

If moreover one requires $\mathcal{I}$ to be topologically closed, one can lower d to having fixed value 24. Finally, an examination of the proof reveals that the theorem also holds for the domain of semialgebraic sets, and in fact for any domain of o-minimal sets in the sense of [1]. The proof also carries through whether one considers the domain of semilinear sets having rational, algebraic, or real coordinates.

Although the above is a negative (undecidability) result, it should be viewed in a positive light; as Monniaux writes in [27], *"We started this work hoping to vindicate forty years of research on heuristics by showing that the existence of polyhedral inductive separating invariants in a system with transitions in linear arithmetic (integer or rational) is undecidable."* Theorem 1 shows that, at least as regards non-convex invariants, the development and use of heuristics is indeed vindicated and will continue to remain essential. Related questions of *completeness* of given abstraction scheme have also been examined by Giaccobazzi *et al.* in [15, 14].

It is important to note that our undecidability result requires at least *two* transitions. In fact, much research work has been expended on the class of simple *affine* loops, *i.e.*, one-location programs equipped with a single self-transition. In terms of invariants, Fijalkow *et al.* establish in [11, 12] the decidability of the existence of *semialgebraic* separating invariants, and specifically state the question of the existence of separating *semilinear* invariants as an open problem. Almagor *et al.* extend this line of work in [1] to more complex targets (in lieu of the point y) and richer classes of invariants. The second main result of the present paper is to settle the open question of [11, 12] in the affirmative:

Theorem 2. *Let $A \in \mathbb{Q}^{d\times d}$ be a rational square matrix of dimension d, and let $x, y \in \mathbb{Q}^d$ be two points in $\mathbb{Q}^d$. It is decidable whether there exists a closed semilinear set $\mathcal{I} \subseteq \mathbb{R}^d$ having algebraic coordinates such that:*

1. *$x \in \mathcal{I}$;*
2. *$A\mathcal{I} \subseteq \mathcal{I}$; and*
3. *$y \notin \mathcal{I}$.*

The proof shows that, in fixed dimension d, the decision procedure runs in polynomial time. It is worth noting that one also has undecidability if A, x, and y are taken to have real-algebraic (rather than rational) entries.

Let us conclude this section by briefly commenting on the important issue of *convexity.* At its inception, abstract interpretation had a marked preference for domains of *convex* invariants, of which the interval domain, the octagon domain, and of course the domain of convex polyhedra are prime examples. Convexity confers several distinct advantages, including simplicity of representation, algorithmic tractability and scalability, ease of implementation, and better termination heuristics (such as the use of widening). The central drawback of convexity, on the other hand, is its poor expressive power. This has been noted time and again: *"convex polyhedra [...] are insufficient for expressing certain invariants, and what is often needed is a disjunction of convex polyhedra."* [2]; *"the ability to express non-convex properties is sometimes required in order to* *achieve a precise analysis of some numerical properties"* [13]. Abstract interpretation can accommodate non-convexity either by introducing disjunctions (see, *e.g.*, [2] and references therein), or via the development of special-purpose domains of non-convex invariants such as *donut domains* [13]. The technology, data structures, algorithms, and heuristics supporting the use of disjunctions in the leading abstract-interpretation tool ASTRÉE are presented in great detail in [8]. In the world of software verification, where predicate abstraction is the dominant paradigm, disjunctions—and hence non-convexity—are nowadays native features of the landscape.

It is important to note that the two main results presented in this paper, Theorems 1 and 2, have only been proven for families of invariants that are not necessarily convex. The Monniaux Problem restricted to families of *convex* invariants remains open and challenging.

2 Preliminaries

2.1 Complex and algebraic numbers

The set of complex numbers is $\mathbb{C}$, and for a complex number z its modulus is $|z|$, its real part is $\mathrm{Re}\,(z)$ and its imaginary part is $\mathrm{Im}\,(z)$. Let $\mathbb{C}^*$ denote the set of non-zero complex numbers. We write S^1 for the complex unit circle, *i.e.* the set of complex numbers of modulus 1. We let $\mathbb{U}$ denote the set of roots of unity, *i.e.* complex numbers $z \in S^1$ such that $z^n = 1$ for some $n \in \mathbb{N}$.

When working in $\mathbb{C}^d$, the norm of a vector z is $||z||$, defined as the maximum of the moduli of each complex number z_i for i in $\{1, \ldots, d\}$. For $\varepsilon > 0$ and z in $\mathbb{C}^d$, we write $B(z, \varepsilon)$ for the open ball centered in z of radius ε. The topological closure of a set $\mathcal{I} \subseteq \mathbb{C}^d$ is $\overline{\mathcal{I}}$, its interior $\mathcal{I}^{\mathrm{o}}$, and its frontier $\partial\mathcal{I}$, defined as $\overline{\mathcal{I}} \cap \overline{\mathbb{C}^d \setminus \mathcal{I}}$.

We will mostly work in the field $\mathbb{A} \subseteq \mathbb{C}$ of algebraic numbers, that is, roots of polynomials with coefficients in $\mathbb{Z}$. It is possible to represent and manipulate algebraic numbers effectively, by storing their minimal polynomial and a sufficiently precise numerical approximation. An excellent reference in computational algebraic number theory is [7]. All standard algebraic operations such as sums, products, root-finding of polynomials, or computing Jordan normal forms of matrices with algebraic entries can be performed effectively.

2.2 Semilinear sets

A set $\mathcal{I} \subseteq \mathbb{R}^d$ is semilinear if it is the set of (real) solutions of some finite Boolean combination of linear inequalities with algebraic coefficients. We give an equivalent definition now using half-spaces and polyhedra. A half-space $\mathcal{H}$ is a subset of $\mathbb{R}^d$ of the form

$$\mathcal{H} = \left\{ z \in \mathbb{R}^d \mid z \cdot u \succ a \right\},$$

for some u in $\mathbb{A}^d$, a in $\mathbb{A} \cap \mathbb{R}$ and $\succ \in \{\geq, >\}$. A polyhedron is a finite intersection of half-spaces, and a semilinear set a finite union of polyhedra.

We then define semilinear sets in $\mathbb{C}^d$, by identifying $\mathbb{C}^d$ with $\mathbb{R}^{2d}$.

We recall some well known facts about semilinear sets which will be useful for our purposes.

Lemma 3 (Projections of Semilinear Sets). *Let $\mathcal{I}$ be a semilinear set in $\mathbb{R}^{d+d'}$. Then the projection of $\mathcal{I}$ on the first d coordinates, defined by*

$$\Pi(\mathcal{I}, d) = \left\{ z \in \mathbb{R}^d \mid \exists t \in \mathbb{R}^{d'}, (z,t) \in \mathcal{I} \right\}$$

is a semilinear set.

Lemma 4 (Sections of Semilinear Sets). *Let $\mathcal{I}$ be a semilinear set in $\mathbb{R}^{d+d'}$ and t in $\mathbb{R}^{d'}$. Then the section of $\mathcal{I}$ along t, defined by*

$$\mathit{Section}(\mathcal{I}, t) = \left\{ z \in \mathbb{R}^d \mid (z,t) \in \mathcal{I} \right\},$$

is a semilinear set.

Furthermore, there exists a bound B in $\mathbb{R}$ such that for all t in $\mathbb{R}^{d'}$ of norm at most 1, if $\mathit{Section}(\mathcal{I}, t)$ is non-empty, then it contains some z in $\mathbb{R}^d$ of norm at most B.

For the reader's intuitions, note that the last part of this lemma does not hold for more complicated sets. For instance, consider the hyperbola defined by $\mathcal{I} = \left\{ (x,y) \in \mathbb{R}^2 \mid xy = 1 \right\}$. Choosing a small x forces to choose a large y, hence there exist no bound B as stated in the lemma for $\mathcal{I}$.

The dimension of a set X of $\mathbb{R}^d$ is the minimal k in $\mathbb{N}$ such that X is included in a finite union of affine subspaces of dimension at most k.

Lemma 5 (Dimension of Semilinear Sets). *Let $\mathcal{I}$ be a semilinear set in $\mathbb{R}^d$. If $\mathcal{I}^{\mathrm{o}} = \emptyset$, then $\mathcal{I}$ has dimension at most $d-1$.*

3 Main results and proof overviews

A dynamical system is given by a set of functions $f_t : \mathbb{R}^d \to \mathbb{R}^d$ for $t \in [1,k]$. Let x be an initial vector, the set of *reachable points* from x is the smallest subset R of $\mathbb{R}^d$ containing x and closed under the functions f_t: if $z \in R$ then $f_t(z) \in R$. If there is a single function ($k = 1$) the set of reachable points from x is called the *orbit* of x under f. We say that y is reachable from x if y belongs to the set of reachable points from x. The reachability problem takes as input a dynamical system and two vectors x, y, and asks whether y is reachable from x.

Natural certificates that y is not reachable from x are separating invariants: an *invariant* is a set $\mathcal{I} \subseteq \mathbb{C}^d$ such that $f_t(\mathcal{I}) \subseteq \mathcal{I}$ for all $t \in [1,k]$. It is *separating* for (x,y) if additionally $x \in \mathcal{I}$ and $y \notin \mathcal{I}$. The following are equivalent:

- there exists a separating invariant.
- y is not reachable from x,

It is clear that the existence of a separating invariant implies that y is not reachable from x. A stronger statement is: the set R of reachable points from x is a separating invariant for (x, y) if and only if y does not belong to R. However the set R may be very complicated, making it not so useful as a separating invariant. We therefore consider restrictions on the class of invariants.

We are in this paper interested in linear dynamical systems and semilinear invariants:

- in a linear dynamical system, the functions f_t are linear: f_t is induced by a square matrix $M_t \in \mathbb{A}^{d \times d}$ with $f_t(z) = z \cdot M_t$;
- a semilinear invariant is a semilinear set and a separating invariant.

The problem we study in this paper is the semilinear invariant problem, which asks whether given a linear dynamical system there exists a semilinear separating invariant. The two following sections give high level overviews of the proofs for our two main results, namely Theorems 1 and 2.

3.1 Undecidability for several matrices

In this section, we sketch the proof of two undecidability results; as an intermediate step and towards the (complicated) proof of Theorem 1, we prove a simpler undecidability result for closed semilinear invariants. We will only sketch proofs in this section and defer the full proofs to Section 4.

We will construct reductions from the ω-Post Correspondence Problem (in short: ω-PCP), an extension of the well-known Post Correspondence Problem to infinite words. For a word w we let $|w|$ denote its length, and for $i \in [1, |w|]$, we write w_i for the letter of w in position i, so $w = w_1 w_2 \dots$. We write $w_{1 \dots n}$ for the prefix of w of length n.

An instance of the ω-PCP is given by two sets of pairs of non-empty words $\left\{(u^i, v^i)\right\}_{i \in [1,p]}$ over some alphabet Σ. The objective is to determine whether there exists an infinite word $w = w_1 w_2 \dots$ over the alphabet $[1, p]$ such that the following equality over infinite words holds: $u^{w_1} u^{w_2} \cdots = v^{w_1} v^{w_2} \dots$, and in that case we say that w is a solution of $(u^i, v^i)_{i \in [1,p]}$. A pair (u^i, v^i) is called a tile, see Figure 1 for a graphical representation.

This problem is known to be undecidable [16] even for a fixed p and an alphabet of size 2. For the remainder of this section, we let p denote the smallest number such that the ω-PCP is undecidable with a fixed number of tiles p. The latest improvement on this result shows that $p \leq 8$ [10].

A first undecidability result for closed semilinear invariants

The first undecidability result we prove is for (topologically) closed invariants: it does not yet imply Theorem 1; the reduction will be further refined later on.

Theorem 6. *The semilinear invariant problem is undecidable for closed invariants with p matrices of dimension* 3.

Let us consider an ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$. Without loss of generality the alphabet is $\Sigma = \{0, 2\}$: this way a word $u = u_1 \ldots u_n \in \Sigma^*$ is encoded as the digits of some real number in $[0, 1]$ in base 4 (with least significant digit to the right):

$$[u] = \sum_{i=1}^{n} u_i 4^{-i}.$$

The choice of base 4 and digits in $\{0, 2\}$ instead of the more canonical base 2 is for having a "sparse" encoding, which will be useful for defining invariants. Figure 1 illustrates the encoding of ω-PCP. A finite word $w \in [1, p]^*$ induces two finite words $u^w, v^w \in \Sigma^*$:

$$u^w = u^{w_1} u^{w_2} \ldots u^{w_n} \quad ; \quad v^w = v^{w_1} v^{w_2} \ldots v^{w_n}.$$

We say that w is a partial solution if either u^w is a prefix of v^w or v^w a prefix of u^w.

We encode w by the vector $([u^w] - [v^w], 4^{-|u^w|}, 4^{-|v^w|})$ of dimension 3. The remarkable property of this encoding is that adding the tile (u^i, v^i) to w, meaning considering wi, corresponds to multiplying the vector by a fixed matrix M_i. Formally, for a tile (u^i, v^i), we construct a 3×3 matrix M_i such that

$$([u^w] - [v^w], 4^{-|u^w|}, 4^{-|v^w|}) \cdot M_i = ([u^{wi}] - [v^{wi}], 4^{-|u^{wi}|}, 4^{-|v^{wi}|}).$$

For a word $w \in [1, p]^*$ we define M_w: it is obtained by multiplying the matrices M_i following w. For instance $M_{13422} = M_1 M_3 M_4 M_2 M_2$. Note that the set of reachable points from x is $\{x \cdot M_w : w \in [1, p]^*\}$.

Let $x = (0, 1, 1)$, the equality above implies that

$$x \cdot M_w = ([u^w] - [v^w], 4^{-|u^w|}, 4^{-|v^w|}).$$

Let $y = (0, 0, 0)$. Let us consider the system $S = (\{M_i\}_{i \in [1,p]}, x, y)$. We now argue the ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$ does not have a solution if and only if there exists a closed separating semilinear invariant for S.

We first show that the existence of a solution implies the non-existence of closed separating invariants. Considering the prefixes of a solution of the ω-PCP yields a sequence of matrices in M which converges to the zero matrix. In other words, in that case y is in the topological closure of the reachable set from x. This implies that there cannot exist a closed separating invariant (semilinear or not).

Conversely, if there is no solution to the ω-PCP instance then an application of König's lemma implies that there exists a bound $N \in \mathbb{N}$ such that there are no partial solutions of length N. It follows that for any $w \in [1, p]^+$ the first coordinate of $x \cdot M_w$, which is $[u^w] - [v^w]$, is lower bounded in absolute value by 4^{-N}. From this observation we can construct a closed separating semilinear invariant (we refer to the full proof for details).

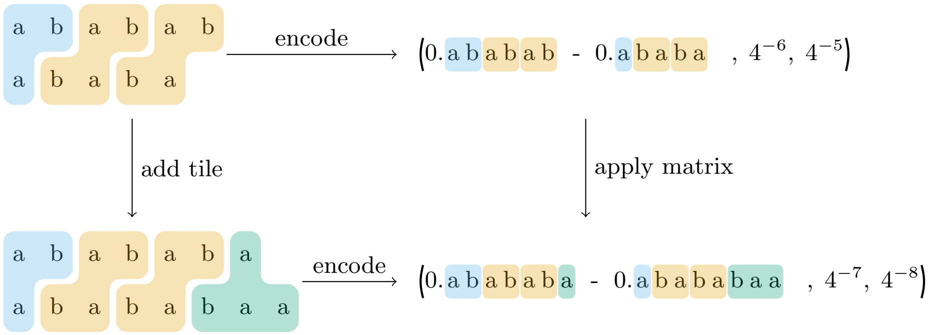

Fig. 1. Encoding using matrices: the partial solution consisting of 3 tiles on the left is encoded as three real numbers on the right (here a and b are digits). For each tile we construct a matrix such that concatenating the tile on the left is equivalent to multiplying this vector by the matrix corresponding to the tile.

The main undecidability result

The above reduction strongly relies on the fact that if the ω-PCP instance has a solution then the target belongs to the closure of the set of reachable points, since this property implies that there cannot exist a *closed* separating invariant. To obtain the undecidability for the class of all semilinear invariants, we refine the reduction above.

Theorem 7. *The semilinear invariant problem is undecidable with* $p+4$ *matrices in dimension* 8.

Reducing to two matrices

In the reductions above we used p matrices in dimension 3×3 and $p+4$ matrices in dimension 8×8. A standard transformation reduces the number of matrices by combining all matrices into one large matrix M and adding a shift matrix M_{shift}, yielding the following result strengthening Theorem 1.

Corollary 8. *The closed semilinear invariant problem is undecidable with* 2 *matrices of dimension* $3p$*, and the semlinear invariant problem is undecidable with* 2 *matrices of dimension* $8(p+4)$.

3.2 Decidability for simple linear loops

In this section, we are only concerned with simple linear loops: an Orbit instance is (A, x, y), and the objective is to determine whether there exists a separating semilinear invariant, meaning a semilinear set $\mathcal{I}$ such that $x \in \mathcal{I}$, $\mathcal{I}\cdot A \subseteq \mathcal{I}$, and $y \notin \mathcal{I}$. Since it is possible to decide (in polynomial time) whether y is in the reachability set from x [18, 19], we may always assume that the answer is negative. All decidability results are only concerned with *closed invariants*, which is crucial in several proofs.

Theorem 2 *There is an algorithm that decides whether an Orbit instance admits a closed semilinear invariant. Furthermore, it runs in polynomial time assuming the dimension d is fixed.*

Before sketching the proof of Theorem 2, we comment a few instructive examples that illustrate the different cases that arise.

Example 9. Consider the Orbit instance $\ell = (A, x, y)$ in dimension 2 where

$$A = \frac{1}{2}\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix},$$

$x = (1, 0)$ and $y = (3, 3)$. The orbit is depicted on Figure 2. Here, A is a counterclockwise rotation around the origin with an expanding scaling factor. A suitable semilinear invariant can be constructed by taking the complement of the convex hull of a large enough number of points of the orbit, and adding the missing points. In this example, we can take

$$\mathcal{I} = \{x, Ax\} \cup \overline{\mathrm{Conv}\left(\{A^n x, n \leq 8\}\right)^{\mathsf{c}}}.$$

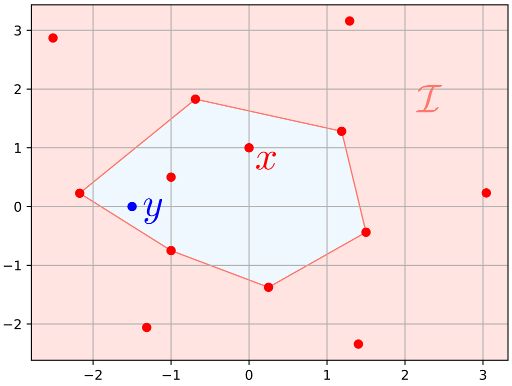

Fig. 2. An invariant for example 9.

Constructing an invariant of this form will often be possible, for instance when A has an eigenvalue of modulus > 1. A similar (yet more involved) construction gives the same result when A has an eigenvalue of modulus < 1.

The case in which all eigenvalues have modulus 1 is more involved. Broadly speaking, invariant properties in such cases are often better described by sets involving equations or inequalities of higher degree [11], which is why interesting semilinear invariants do not exist in many instances. However, delineating exactly which instances admit separating semilinear invariants is challenging, and is our main technical contribution on this front. The following few examples illustrate some of the phenomena that occur.

Example 10. Remove the expanding factor from the previous instance, that is, put instead

$$A = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}.$$

Now A being a rotation of an irrational angle, the orbit of x is dense in the circle of radius 1. It is quite easy to prove that no semilinear invariant exists (except for the whole space $\mathbb{R}^2$) for this instance, whatever the value of y. This gives a first instance of non-existence of a semilinear invariant. Many such examples exist, and we shall now supply a more subtle one. Note that simple invariants do exist, such as the unit circle, which is a semialgebraic set but not a semilinear one.

Example 11. Consider $\ell = (A, x, y)$ in dimension 4 with

$$A = \begin{bmatrix} A' & I_2 \\ 0 & A' \end{bmatrix},$$

where A' is the matrix from Example 10, $x = (0, 0, 1, 0)$ and y is arbitrary. When repeatedly applying A to x, the last two coordinates describe a circle of radius 1 as in the previous example. However, the first two coordinates diverge: at each step, they are rotated and the last two coordinates are added. In this instance, no semilinear invariant exists (except again for the whole space $\mathbb{R}^4$), however proving this is somewhat involved. Note however once more that non-trivial semialgebraic invariants may easily be constructed.

In examples 10 and 11, no non-trivial semilinear invariant exist, or equivalently any semilinear invariant must contain $\mathcal{I}_0$, where $\mathcal{I}_0$ is the whole space. In all instances for which constructing an invariant is not necessarily immediate (as is the case in Example 9), we will provide a minimal invariant, that is, a semilinear invariant $\mathcal{I}_0$ with the property that any semilinear invariant will have to contain $\mathcal{I}_0$. In such cases there exists a semilinear invariant (namely $\mathcal{I}_0$) if and only if $y \notin \mathcal{I}_0$. We conclude this discussion with two examples having such minimal semilinear invariants.

Example 12. Consider $\ell = (A, x, y)$ in dimension 3 with

$$A = \begin{bmatrix} A' & 0 \\ 0 & -1 \end{bmatrix},$$

where A' is the matrix of Example 10, a 2-dimensional rotation by an angle which is not a rational multiple of 2π and $x = (1, 0, 1)$. As we iterate matrix A, the two first coordinates describe a circle, and the third coordinate alternates between 1 and -1: the orbit is dense in the union of two parallel circles. In this example, the minimal semilinear invariant is the union of the two planes containing these circles.

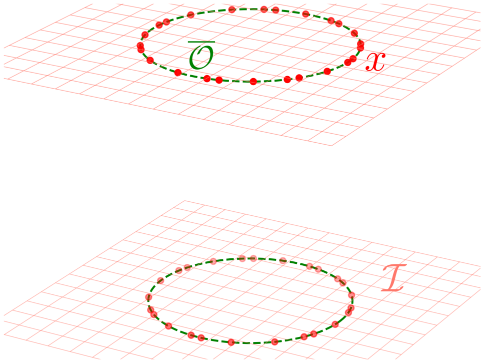

Fig. 3. The minimal invariant for Example 12. Here, $\bar{\mathcal{O}}$ denotes the topological closure of the orbit of x.

Example 13. Consider $\ell = (A, x, y)$ in dimension 8 with

$$A = \begin{bmatrix} A' & 0 \\ 0 & -A' \end{bmatrix},$$

where A' is the matrix from Example 11. This can be seen as two instances of Example 11 running in parallel. Let $x = (0, 0, 1, 0, 0, 0, -7, 0)$, and note that both blocks of x are initially related by a multiplicative factor, namely $-7(x_1, x_2, x_3, x_4) = (x_5, x_6, x_7, x_8)$. Moreover, as the first block is multiplied by the matrix A' while the second one is multiplied by $-A'$, the multiplicative factor relating the two blocks alernates between 7 and -7. Hence,

$$\mathcal{I}_0 = \{u \in \mathbb{R}^8 \mid (u_1, u_2, u_3, u_4) = \pm 7(u_5, u_6, u_7, u_8)\},$$

is an invariant, which one can prove to be the minimal semilinear invariant. Note that I_0 has dimension 4. If however, we let $x = (0, 0, 1, 0, 1, 0, -7, 0)$, then the minimal semilinear invariant becomes

$$\{u \in \mathbb{R}^8 \mid (u_3, u_4) = \pm 7(u_7, u_8)\},$$

which has dimension 6. Roughly speaking, no semilinear relation holds between (u_1, u_2) and (u_5, u_6).

We shall now give a detailed overview of the proof of Theorem 2 while avoiding technicalities and details. We point to Section 5 for full proofs. Recall that we only consider closed semilinear invariants. Let us describe the general strategy.

- We first normalize the Orbit instance, which amounts to putting matrix A in Jordan normal form, and dealing with some easy instances.
- We then eliminate some positive cases. More precisely, we construct invariants whenever one of the three following conditions is realized:
  - A has an eigenvalue of modulus > 1.
  - A has an eigenvalue of modulus < 1.
  - A has a Jordan block of size ≥ 2 with an eigenvalue that is a root of unity.
- We are now left with an instance where all eigenvalues are of modulus 1 and not roots of unity, which is the most involved part of the paper. In this setting, we exhibit the minimal semilinear invariant $\mathcal{I}$ containing x. In particular, there exists a semilinear invariant (namely, $\mathcal{I}$) if and only if $y \notin \mathcal{I}$.

Normalization As a first step, recall that every matrix A can be written in the form $A = Q^{-1}JQ$, where Q is invertible and J is in Jordan normal form. The following lemma transfers semilinear invariants through the change-of-basis matrix Q.

Lemma 14. *Let $\ell = (A, x, y)$ be an Orbit instance, and Q an invertible matrix in $\mathbb{A}^{d\times d}$. Construct the Orbit instance $\ell_Q = (QAQ^{-1}, Qx, Qy)$. Then $\mathcal{I}$ is a semilinear invariant for ℓ_Q if, and only if, $Q^{-1}\mathcal{I}$ is a semilinear invariant for ℓ.*

Proof. First of all, $Q^{-1}\mathcal{I}$ is semilinear if, and only if, $\mathcal{I}$ is semilinear. Then

- $QAQ^{-1}\mathcal{I} \subseteq \mathcal{I}$ if, and only if, $AQ^{-1}\mathcal{I} \subseteq Q^{-1}\mathcal{I}$,
- $Qx \in \mathcal{I}$ if, and only if, $x \in Q^{-1}\mathcal{I}$,
- $Qy \notin \mathcal{I}$, if, and only if, $y \notin Q^{-1}\mathcal{I}$.

This concludes the proof.

Thanks to Lemma 14, one may reduce the problem of the existence of semilinear invariants for Orbit instances to cases in which the matrix is in Jordan normal form, *i.e.*, is a diagonal block matrix, where the blocks (called Jordan blocks) are of the form:

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

Note that this transformation can be achieved in polynomial time [3, 4]. Formally, a Jordan block is a matrix $\lambda I + N$ with $\lambda \in \mathbb{C}$, I the identity matrix and N the matrix with 1's on the upper diagonal, and 0's everywhere else. The number λ is an eigenvalue of A. We will use notation $\mathcal{J}_d(\lambda)$ for the Jordan block of size d

with eigenvalue λ. A Jordan block of dimension one is called diagonal, and A is diagonalisable if, and only if, all Jordan blocks are diagonal.

The d positions in the matrix A are indexed by pairs (J, k), where J ranges over the Jordan blocks and $k \in \{1, \ldots, d(J)\}$, $d(J)$ being the dimension of the Jordan block J. For instance, if the matrix A has two Jordan blocks, J_1 of dimension 1 and J_2 of dimension 2, then the three dimensions of A are $(J_1, 1)$ and $(J_2, 1), (J_2, 2)$.

For a point v and a subset S of positions, we let v_S be the projection of v on the positions in S, and extend this notation to matrices. For instance, v_J is the point corresponding to the dimensions of the Jordan block J, and $v_{J,>k}$ is its projection on the coordinates of the Jordan block J whose indices are greater than k. We write S^{c} for the positions which are not in S.

There are a few degenerate cases which are handled separately. We say that an Orbit instance $\ell = (A, x, y)$ is normalized if:

- The matrix A is in Jordan normal form.
- There is no Jordan block associated with the eigenvalue 0, or equivalently A is invertible.
- For each Jordan block J, the last coordinate of the point x_J is not zero, *i.e.* $x_{J,d(J)} \neq 0$.
- There is no diagonal Jordan block with an eigenvalue which is a root of unity,
- Any Jordan block J with an eigenvalue of modulus < 1 has $y_J \neq 0$.

Lemma 15. *The existence of semilinear invariants for Orbit instances reduces to the same problem for normalized Orbit instances in Jordan normal form.*

We refer to Section 5 for a formal proof of Lemma 15.

Positive cases Many Orbit instances present a divergence which one may exploit to construct a semilinear invariant. Such behaviours are easily identified once the matrix is in Jordan normal form. We isolate three such cases. All details are presented in Section 5.

- If there is an eigenvalue of modulus > 1. Call J its Jordan block. Projecting to the last coordinate of J the orbit of x diverges to ∞ in modulus (see Example 9). A long enough "initial segment" $\{x, Ax, \ldots, A^k x\}$ of the orbit, together with the complement of its convex hull (on the last coordinate of J) constitutes a semilinear invariant.
- If there is an eigenvalue of modulus < 1 in block J, the situation is quite similar with a convergence towards 0. However, the construction we give is more involved, the reason being that we may not just concentrate on the last nonzero coordinate $x_{J,l}$ of x_J, since $y_{J,l}$ may very well be 0, the limit of $(A^n x)_{J,l}$. Yet on the full block, $(A^n x)_J$ goes to zero while $y_J \neq 0$. We show how to construct, for any $0 < \varepsilon$, a semilinear invariant $\mathcal{I}$ such that $B(0, \varepsilon') \subseteq \mathcal{I} \subseteq B(0, \varepsilon)$ for some $\varepsilon' > 0$. Picking ε small enough we make sure that $y \notin \mathcal{I}$, and then $\{x, Ax, \ldots, A^k x\} \cup \mathcal{I}$ is a semilinear invariant if k is large enough so that $||A^k x|| \leq \varepsilon'$.

- Finally, if there is an eigenvalue which is a root of unity, say $\lambda^n = 1$, on a Jordan block J of size at least 2 (that is, a non diagonal block), then the penultimate coordinate on J of the orbit goes to ∞ in modulus. In this case, the orbit on this coordinate is contained in a union of n half-lines which we cut far enough away from 0 and add an initial segment to, in order to build a semilinear invariant.

Note that in each of these cases, we isolate a Jordan block, concentrate on the corresponding (stable) eigenspace, construct a separating semilinear invariant for this projection of the problem, and extend it to the full space by allowing any value on other coordinates.

Minimal invariants We have now reduced to an instance where all eigenvalues have modulus 1 and are not roots of unity. Intuitively, in this setting, semilinear invariants fail, as they are not precise enough to exploit subtle multiplicative relations that may hold among eigenvalues. However, it may be the case that some coarse information in the input can still be stabilised by a semilinear invariant, for instance if two synchronised blocks have some identical components (see Examples 12 and 13).

We start by identifying exactly where semilinear invariants fail. Call two eigenvalues equivalent if their quotient is a root of unity. Informally, if λ_1 and λ_2 are equivalent, *e.g.* $\lambda_1^n = \lambda_2^n$, then for all k, it holds that $\lambda_1^k \in \{e^{\frac{2i\pi}{n}}\lambda_2^k, 0 \leq i \leq n-1\}$, which may be exploited to construct non-trivial semilinear invariants. We show however that whenever no two different eigenvalues are equivalent, the only stable semilinear sets are trivial. This lower bound (non-existence of non-trivial semilinear invariant) constitutes the most technically involved part. Our proof is inductive with as base case the diagonal case, where it makes crucial use of the Skolem-Mahler-Lech theorem.

When the matrix has several equivalent eigenvalues, we show how to iteratively reduce the dimension in order to eventually fall into the previous scenario. Very roughly speaking, if A is comprised of two identical blocks B, we show that it suffices to compute a minimal invariant $\mathcal{I}_B$ for B, since $\{z \mid \tilde{z}_1 \in \mathcal{I}_B \text{ and } \tilde{z}_2 = \tilde{z}_1\}$ (with obvious notations) is a minimal invariant for A. This is achieved, by first assuming that all equivalent eigenvalues are in fact equal and then easily reducing to this case by considering a large enough iterations of A.

All details are presented in Section 5.

4 Undecidability proofs

The structure of this section follows the outline given in Section 3, we rely on the explanations given there but state and prove all technical details here.

4.1 Proof of Theorem 6

We start with proving Theorem 6: the semilinear invariant problem is undecidable for closed invariants with p matrices of dimension 3. We refer to Subsection 3.1 for the definition of ω-PCP, a sketch of the proofs, and the statements. Recall that p is the smallest number such that the ω-PCP is undecidable with a fixed number of tiles p for an alphabet of size 2; we know that $p \leq 8$ [10].

Let us consider an ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$ over some alphabet Σ of size 2. A finite word $w \in [1,p]^*$ induces two finite words $u^w, v^w \in \Sigma^*$:

$$u^w = u^{w_1} u^{w_2} \ldots u^{w_n} \ ; \ v^w = v^{w_1} v^{w_2} \ldots v^{w_n}.$$

We say that w is a partial solution if either u^w is a prefix of v^w or v^w a prefix of u^w. We state (and prove for the sake of completeness) a classical lemma on ω-PCP.

Lemma 16. *Let $(u^i, v^i)_{i \in [1,p]}$ be an ω-PCP instance and $w \in [1,p]^\omega$.*

- *The infinite word $w \in [1,p]^\omega$ is a solution if and only if all prefixes of w are partial solutions.*
- *If there are no solutions, then there exists a bound N such that all partial solutions have length at most N.*

Proof. The first item is clear, so we focus on the second. We consider the infinite tree with branching $[1,p]$: the set of nodes is $[1,p]^*$. We remove from the tree a node w if w is not a partial solution (note that we remove all of the descendants of w since they are also not partial solutions). Since the ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$ does not have a solution, there are no infinite paths in this tree. The tree is finitely branching, so König's lemma implies that it is finite. Let N be the depth of this finite tree, then there are no partial solutions of length greater than N.

Let us write 0 and 2 for the two letters in Σ, meaning $\Sigma = \{0, 2\}$: this way a word $u = u_1 \ldots u_n \in \Sigma^*$ is encoded as the digits of some real number in $[0,1]$ in base 4 (with least significant digit to the right):

$$[u] = \sum_{i=1}^{n} u_i 4^{-i}.$$

The choice of base 4 and digits in $\{0, 2\}$ instead of the more canonical base 2 is for having a "sparse" encoding as explained later. We encode $w \in [1,p]^*$ by the vector $([u^w] - [v^w], 4^{-|u^w|}, 4^{-|v^w|})$ of dimension 3. The remarkable property of this encoding is that adding the tile (u^i, v^i) to w, meaning considering wi, corresponds to multiplying the vector by the following matrix M_i:

$$M_i = \begin{bmatrix} 1 & 0 & 0 \\ [u^i] & 4^{-|u_i|} & 0 \\ -[v^i] & 0 & 4^{-|v_i|} \end{bmatrix}.$$

For $w \in [1,p]^\omega$, we write $w_{1\ldots n}$ for the prefix of length n of w. For $w \in [1,p]^*$ we define M_w as follows: M_w is obtained by multiplying the matrices M_i following w, for instance $M_{13422} = M_1 M_3 M_4 M_2 M_2$.

Let $x = (0, 1, 1)$. We state in the following lemma the key properties of the encoding.

Lemma 17. *Let $(u^i, v^i)_{i \in [1,p]}$ be an ω-PCP instance.*

1. *Let $w \in [1,p]^*$, we have $x \cdot M_w = ([u^w] - [v^w], 4^{-|u^w|}, 4^{-|v^w|})$.*
2. *Let us write $x \cdot M_w = (s, c, d)$. Then:*
   - *If w is a partial solution then $|s| \leq \frac{2}{3}(c + d)$.*
   - *If w is not a partial solution then $|s| > \frac{2}{3}(c + d)$.*
3. *Let $z = (s, c, d)$ and $\alpha \geq 0$. Let us write $z \cdot M_i = (s', c', d')$ for some $i \in [1,p]$. If $|s| \geq \frac{2}{3}(c + d) + \alpha$, then $|s'| \geq \frac{2}{3}(c' + d') + \alpha$.*

Proof. We prove the three items.

1. The calculation for $x \cdot M_w$ is done by induction on w, noting that:
$$([u^w] - [v^w], 4^{-|u^w|}, 4^{-|v^w|}) \cdot M_i = ([u^w u_i] - [v^w v_i], 4^{-|u^w u_i|}, 4^{-|v^w v_i|}),$$
since $[u^w u_i] = [u^w] + 4^{-|u^w|}[u_i]$ and $[v^w v_i] = [v^w] + 4^{-|v^w|}[v_i]$.
2. Let $x \cdot M_w = (s, c, d)$.
   - Assume that w is a partial solution: either u^w is a prefix of v^w, or the other way around. Assume the former holds: we have $v^w = u^w u'$ for some u'. This implies that $[v^w] = [u^w] + 4^{-|u^w|}[u']$. Since $[u'] \leq 1$, we obtain
   $$|s| = |[v^w] - [u^w]| \leq 4^{-|u^w|} = c.$$
   In the other case, the same reasoning yields $|s| \leq d$. Thus $|s| \leq \frac{1}{2}(c+d) \leq \frac{2}{3}(c + d)$.
   - Assume that w is not a partial solution, and let us write n for the smallest position such that $u^w_n \neq v^w_n$. Then
   $$[u^w] - [v^w] = (u^w_n - v^w_n)\frac{1}{4^n} + \sum_{j \geq n+1} \left(u^w_j - v^w_j\right)\frac{1}{4^j}.$$
   The choice of base 4 and digits in $\{0, 2\}$ is all contained in the following calculations. Since $u^w_n \neq v^w_n$ and they are digits in $\{0, 2\}$, we have $|u^w_n - v^w_n| = 2$. For $j \geq n + 1$ we have $|u^w_j - v^w_j| \leq 2$ so
   $$\left| \sum_{j \geq n+1} (u^{wi}_j - v^{wi}_j)\frac{1}{4^j} \right| < \frac{2}{4^{n+1}} \cdot \sum_{j \geq 0} \frac{1}{4^j} = \frac{2}{3} \cdot \frac{1}{4^n}.$$
   It follows that
   $$\begin{aligned} |s| = |[u^w] - [v^w]| &> 2 \cdot \frac{1}{4^n} - \frac{2}{3} \cdot \frac{1}{4^n} \\ &= \frac{4}{3} \cdot \frac{1}{4^n} \\ &\geq \frac{2}{3}(c + d). \end{aligned}$$
   In the last inequality we use $n \leq |u^w|$ and $n \leq |v^w|$.

3. Let $z = (s, c, d)$ and $z \cdot M_i = (s', c', d')$ for some $i \in [1, p]$. Assume that $|s| \geq \frac{2}{3}(c + d) + \alpha$.

$$\begin{aligned} |s'| = |s + c[u^i] - d[v^i]| &\geq |s| - c[u^i] - d[v^i] \\ &\geq \tfrac{2}{3}(c+d) + \alpha - c[u^i] - d[v^i] \\ &= \underbrace{\left(\frac{2}{3} - [u^i]\right)}_{\geq \frac{2}{3} \cdot 4^{-|u^i|}} c + \underbrace{\left(\frac{2}{3} - [v^i]\right)}_{\geq \frac{2}{3} \cdot 4^{-|v^i|}} d + \alpha \\ &\geq \tfrac{2}{3}(c' + d') + \alpha. \end{aligned}$$

We have used the inequality $\frac{2}{3} - [u] \geq \frac{2}{3} \cdot 4^{-|u|}$, valid for $|u| \geq 1$. Thus $|s'| \geq \frac{2}{3}(c' + d') + \alpha$.

Let $y = (0, 0, 0)$. We construct the linear dynamical system $S = (\{M_i\}_{i \in [1,p]}, x, y)$.

Lemma 18. *The ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$ does not have a solution if and only if there exists a closed separating semilinear invariant for S.*

Proof. We distinguish two cases.

- Either the ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$ has a solution $w \in [1, p]^\omega$. Thanks to Lemma 17 we have

$$x \cdot M_{w_{1 \dots n}} = ([u^{w_{1 \dots n}}] - [v^{w_{1 \dots n}}], 4^{-|u^{w_{1 \dots n}}|}, 4^{-|v^{w_{1 \dots n}}|}).$$

  Since w is a solution, $w_{1 \dots n}$ is a partial solution, so again thanks to Lemma 17:

$$|[u^{w_{1 \dots n}}] - [v^{w_{1 \dots n}}]| \leq \frac{2}{3}\left(4^{-|u^{w_{1 \dots n}}|} + 4^{-|v^{w_{1 \dots n}}|}\right),$$

  implying that $\lim_n x \cdot M_{w_{1 \dots n}} = (0, 0, 0) = y$. In other words, $y \in \overline{\{x \cdot M_w : w \in [1, p]^*\}}$, the topological closure of the set of reachable points from x.
  Note that an invariant set $\mathcal{I}$ for S containing x also contains the set of reachable points from x. If additionally $\mathcal{I}$ is closed, then it contains its closure, hence it contains y. Thus there are no semilinear invariants for S. (Note that we did not use semilinarity here.)
- Or the ω-PCP instance $(u^i, v^i)_{i \in [1,p]}$ does not have a solution. Thanks to Lemma 16 there exists a bound N such that all partial solutions have length less than N. Let

$$\alpha = \min \left\{ |s| - \frac{2}{3}(c + d) : x \cdot M_w = (s, c, d) \text{ and } |w| = N \right\},$$

  thanks to Lemma 17 we have $\alpha > 0$.
  Let us define the sets

$$\begin{aligned} \mathcal{I}_1 &= \{x \cdot M_w : |w| < N\}, \\ \mathcal{I}_2 &= \left\{(s, c, d) : |s| \geq \tfrac{2}{3}(c + d) + \alpha\right\}, \\ \mathcal{I} &= \mathcal{I}_1 \cup \mathcal{I}_2. \end{aligned}$$

We argue that $\mathcal{I}$ is a separating closed semilinear invariant. It is easy to see that $\mathcal{I}$ is closed, semilinear, contains x, and does not contain y. We show that $\mathcal{I}$ is indeed an invariant: let $z \in \mathcal{I}$, we show that $z \cdot M_i \in \mathcal{I}$. We distinguish two cases.

- Either $z \in \mathcal{I}_1$, meaning $z = x \cdot M_w$ for $|w| < N$. Then $z \cdot M_i = x \cdot M_{wi}$. If $|w| < N - 1$, then $|wi| < N$, so $z \cdot M_i = x \cdot M_{wi} \in \mathcal{I}_1$. Otherwise $|wi| = N$, let us write $z \cdot M_i = (s, c, d)$. Since there are no partial solutions of length N, thanks to Lemma 17 and the definition of α we have $|s| \geq \frac{2}{3}(c + d) + \alpha$. This shows that $z \cdot M_i \in \mathcal{I}_2$.
- Or $z \in \mathcal{I}_2$. Thanks to Lemma 17 we have $z \cdot M_i \in \mathcal{I}_2$.

4.2 Proof of Theorem 7

For technical convenience it will be useful to use affine transitions instead of linear ones; an affine transition is of the form $z \leftarrow z \cdot M + a$ for a matrix M and a vector a. A classical transformation reduces affine transitions to linear ones by adding a single dimension, as stated in the following lemma.

Lemma 19. *Let S a dynamical system with affine transitions in dimension d, we can construct a linear dynamical system S' such that there exists a (semilinear) separating invariant for S if and only if there exists a (semilinear) separating invariant for S'.*

We work in dimension 7, and divide a vector $z = (s, c, d, n, u, v, m)$ in two blocks: (s, c, d, n) and (u, v, m). Let us define operations on each block:

- Resetting (s, c, d, n) is to perform the following operations, abbreviated $\text{Reset}(s, c, d, n)$:

$$s \leftarrow 0 \;;\; c \leftarrow 1 \;;\; d \leftarrow 1 \;;\; n \leftarrow 0.$$

  We say that (s, c, d, n) is "reset" if $(s, c, d, n) = (0, 1, 1, 0)$.
- Simulating i on (s, c, d, n) is to perform the following operations, abbreviated $\text{Simulation}_i(s, c, d, n)$, where $m = \max(|u_i|, |v_i|)$:

$$s \leftarrow 4^m (s + [u_i]c - [v_i]d) \;;\; c \leftarrow 4^{m-|u_i|}c \;;\; d \leftarrow 4^{m-|v_i|}d \;;\; n \leftarrow n + 2.$$

- Resetting (u, v, m) is to perform the following operations, abbreviated $\text{Reset}(u, v, m)$:

$$u \leftarrow 0 \;;\; v \leftarrow 0 \;;\; m \leftarrow 0.$$

  We say that (u, v, m) is "reset" if $(u, v, m) = (0, 0, 0)$.

We can now define the transitions.

- For each $i \in [1, p]$, the transition t_i does the following: $\text{Simulation}_i(s, c, d, n) \;;\; \text{Reset}(u, v, m)$.
- The transition t_{transfer} does the following: $u \leftarrow 3s - 2c - 2d \;;\; v \leftarrow -3s - 2c - 2d \;;\; m \leftarrow n \;;\; \text{Reset}(s, c, d, n)$.
- The transition $t_{\text{increase}(u)}$ does the following: $\text{Reset}(s, c, d, n) \;;\; u \leftarrow u + 1$.
- The transition $t_{\text{increase}(v)}$ does the following: $\text{Reset}(s, c, d, n) \;;\; v \leftarrow v + 1$.

- The transition $t_{\text{decrease}(m)}$ does the following: $\text{Reset}(s,c,d,n)$; $m \leftarrow m-2$.

For a word $w \in [1,p]^*$ we write t_w for the composition of the transitions t_i following w: for instance $t_{1423} = t_1 t_4 t_2 t_3$.

Let $\widehat{x} = (0,1,1,0,0,0,0)$ and $\widehat{y} = (0,1,1,0,0,0,1)$. We consider the system

$$\widehat{S} = \left(\{t_i : i \in [1,p]\} \cup \left\{t_{\text{transfer}}, t_{\text{increase}(u)}, t_{\text{increase}(v)}, t_{\text{decrease}(m)}\right\}, \widehat{x}, \widehat{y}\right).$$

Lemma 20. *The ω-PCP instance $(u^i,v^i)_{i\in[1,p]}$ does not have a solution if and only if there exists a separating semilinear invariant for $\widehat{S}$.*

Since $\widehat{S}$ uses affine transitions in dimension 7, we obtain an equivalent system using linear transitions in dimension 8 using Lemma 19.

Proof. We distinguish two cases.

- Either the ω-PCP instance $(u^i,v^i)_{i\in[1,p]}$ has a solution $w \in [1,p]^\omega$. Let us consider a semilinear invariant $\mathcal{I}$ for $\widehat{S}$ containing $\widehat{x}$, and show that it necessarily contains $\widehat{y}$.
  Let us consider the set $\mathcal{I}' = \{m \in \mathbb{R} : (0,1,1,0,0,0,m) \in \mathcal{I}\}$. It is semilinear by closure under sections (Lemma 4). We argue that it contains all even natural numbers.
  Let $n \in \mathbb{N}$. Starting from $\widehat{x}$ and applying the transitions $t_{w_1}, t_{w_2}, \ldots, t_{w_n}$ we reach $(s_n, c_n, d_n, 2n, 0, 0, 0)$ with $s_n, c_n, d_n \in \mathbb{Z}$ satisfying $|s_n| \leq \frac{2}{3}(c_n + d_n)$. Then applying the transition t_{transfer} we obtain $(0,1,1,0,u_n,v_n,2n)$ with $u_n, v_n \in \mathbb{Z}$ satisfying $u_n \leq 0$ and $v_n \leq 0$. From there applying the transitions $t_{\text{increase}(u)}$ exactly $-u_n$ times and $t_{\text{increase}(v)}$ exactly $-v_n$ times yields $(0,1,1,0,0,0,2n)$. Since $\mathcal{I}$ is invariant and contains x this implies that $(0,1,1,0,0,0,2n) \in \mathcal{I}$, so $2n \in \mathcal{I}'$.
  Since any infinite semilinear set over the reals must contain an odd natural number, it follows that $\mathcal{I}$ contains $(0,1,1,0,0,0,2m+1)$ for some $m \in \mathbb{N}$. Applying the transition $t_{\text{decrease}(m)}$ exactly m times this implies that $\mathcal{I}$ contains $\widehat{y} = (0,1,1,0,0,0,1)$. Thus there are no separating semilinear invariants for $\widehat{S}$.
- Or the ω-PCP instance $(u^i,v^i)_{i\in[1,p]}$ does not have a solution. Thanks to Lemma 16, there exists a bound N such that all partial solutions have length less than N. Let us define

  $$\begin{aligned}
  \mathcal{I}_1 &= \{t_w(\widehat{x}) : w \in [1,p]^* \text{ with } |w| < N, \text{ and } (u,v,m) \text{ is reset}\},\\
  \mathcal{I}_2 &= \left\{z : |s| > \tfrac{2}{3}(c+d) \text{ and } (u,v,m) \text{ is reset}\right\},\\
  \mathcal{I}_3 &= \{z : (m \leq 0 \text{ or } m \in 2\cdot[0,N] \text{ or } u > 0 \text{ or } v > 0), \text{ and } (s,c,d,n) \text{ is reset}\},\\
  \mathcal{I} &= \mathcal{I}_1 \cup \mathcal{I}_2 \cup \mathcal{I}_3.
  \end{aligned}$$

  We argue that $\mathcal{I}$ is a separating semilinear invariant for $\widehat{S}$. First $\mathcal{I}$ is semilinear, contains $\widehat{x}$ (because $\mathcal{I}_1$ does) and not $\widehat{y}$.
  We show that $\mathcal{I}$ is invariant. Let $z = (s,c,d,n,u,v,m) \in \mathcal{I}$, in the following case distinction we write $t(z) = (s',c',d',n',u',v',m')$. We distinguish three cases, and for each consider all types of transitions:

- If $z \in \mathcal{I}_1$, then $z = t_w(\widehat{x})$ for some $w \in [1,p]^*$ with $|w| < N$.
  - For $i \in [1,p]$, we have $t_i(z) \in \mathcal{I}_1$ or $t_i(z) \in \mathcal{I}_2$: if $|w| < N-1$ then $t_i(z) = t_{wi}(\widehat{x}) \in \mathcal{I}_1$ since $|wi| < N$, otherwise $|wi| = N$ and since there are no partial solutions of length N, wi is not a partial solution so thanks to Lemma 17 we have $|s'| > \frac{2}{3}(c'+d')$, implying that $t_i(z) \in \mathcal{I}_2$.
  - We have $t_{\text{transfer}}(z) \in \mathcal{I}_3$: since $n \in 2 \cdot [0,N]$ we have $m' = n \in 2 \cdot [0,N]$.
  - We have $t_{\text{increase}(u)}(z) \in \mathcal{I}_3$: we have $m = 0$ so $m' = 0$.
  - We have $t_{\text{increase}(v)}(z) \in \mathcal{I}_3$: we have $m = 0$ so $m' = 0$.
  - We have $t_{\text{decrease}(m)}(z) \in \mathcal{I}_3$: we have $m = 0$ so $m' = -2$.
- If $z \in \mathcal{I}_2$, then $|s| > \frac{2}{3}(c+d)$.
  - For $i \in [1,p]$, we have $t_i(z) \in \mathcal{I}_2$: thanks to Lemma 17.
  - We have $t_{\text{transfer}}(z) \in \mathcal{I}_3$: either $u' > 0$ or $v' > 0$.
  - We have $t_{\text{increase}(u)}(z) \in \mathcal{I}_3$: we have $m = 0$ so $m' = 0$.
  - We have $t_{\text{increase}(v)}(z) \in \mathcal{I}_3$: we have $m = 0$ so $m' = 0$.
  - We have $t_{\text{decrease}(m)}(z) \in \mathcal{I}_3$: we have $m = 0$ so $m' = -2$.
- If $z \in \mathcal{I}_3$, then $m \leq 0$ or $(m \in 2 \cdot [0,N])$ or $u > 0$ or $v > 0$.
  - For $i \in [1,p]$, we have $t_i(z) \in \mathcal{I}_1$: indeed $t_i(z) = t_i(\widehat{x})$.
  - We have $t_{\text{transfer}}(z) \in \mathcal{I}_3$: indeed $n = 0$ so $m' = 0$.
  - We have $t_{\text{increase}(u)}(z) \in \mathcal{I}_3$: indeed $m \leq 0$ or $m \in 2 \cdot [0,N]$ or $u > 0$ or $v > 0$, so $m' \leq 0$ or $m' \in 2 \cdot [0,N]$ or $u' > 0$ or $v' > 0$.
  - We have $t_{\text{increase}(v)}(z) \in \mathcal{I}_3$: indeed $m \leq 0$ or $m \in 2 \cdot [0,N]$ or $u > 0$ or $v > 0$, so $m' \leq 0$ or $m' \in 2 \cdot [0,N]$ or $u' > 0$ or $v' > 0$.
  - We have $t_{\text{decrease}(m)}(z) \in \mathcal{I}_3$: indeed $m \leq 0$ or $m \in 2 \cdot [0,N]$, so $m' \leq 0$ or $m \in 2 \cdot [0,N-1]$.

It follows that $\mathcal{I}$ is a semilinear invariant for $\widehat{S}$.

4.3 Proof of Corollary 8

Consider a linear dynamical system $S_d = (\{M_i\}_{i \in [1,p]}, x, y)$ in dimension d, we construct a second linear dynamical system $S_{pd} = (\{M, M_{\text{shift}}\}, x', y')$ in dimension pd using only two transitions such that there exists a (closed, semilinear) separating invariant for S_d if and only if there exists a (closed, semilinear) separating invariant for S_{pd}.

We let I_d denote the identity matrix of size $d \times d$, $0_{d,d'}$ the zero matrix of size $d \times d'$, and 0_d the zero vector of size d. In particular for $d' = 1$ we write 0_d for the zero vector of size d. We now define M and M_{shift}:

$$M = \begin{bmatrix} M_1 & \cdots & 0 \\ & M_2 & \vdots \\ \vdots & \ddots & \\ 0 & \cdots & M_p \end{bmatrix} \quad M_{\text{shift}} = \begin{bmatrix} 0_{d,d} & I_d & & 0_{d,d} \\ & & \ddots & \\ & & & I_d \\ I_d & & & 0_{d,d} \end{bmatrix}.$$

For $z \in \mathbb{R}^d$ and $i \in [1, p]$, the i^{th} shift $z^{\downarrow i} \in \mathbb{R}^{pd}$ of z is

$$z^{\downarrow i} = \begin{bmatrix} 0_{d(i-1)} \\ z \\ 0_{d(p-i)} \end{bmatrix}.$$

Note that $z^{\downarrow i} \cdot M_{\text{shift}} = z^{\downarrow (i \mod p)+1}$, justifying the name "shift".

We let $x' = x^{\downarrow 1}$ and $y' = y^{\downarrow 1}$.

Lemma 21. *Let S_d a linear dynamical system, the linear dynamical system S_{pd} constructed above satisfies the following: there exists a (closed, semilinear) separating invariant for S_d if and only if there exists a (closed, semilinear) separating invariant for S_{pd}.*

Proof. Let $\mathcal{I}$ be a separating invariant for S_d. Let

$$\mathcal{J} = \bigcup_{i=1}^{p} \left\{ z^{\downarrow i} \in \mathbb{R}^{pd} : z \in \mathcal{I} \right\}.$$

We argue that $\mathcal{J}$ is a separating invariant for S_{pd} Clearly $x' \in \mathcal{J}$ and $y' \notin \mathcal{J}$. Let $z^{\downarrow i} \in \mathcal{J}$ for $i \in [1, p]$, then $z^{\downarrow i} \cdot M_{\text{shift}} = z^{\downarrow (i \mod p)+1}$, which is in $\mathcal{J}$, and $z^{\downarrow i} \cdot M = (z \cdot M_i)^{\downarrow i} \in \mathcal{J}$ is also in $\mathcal{J}$. Thus $\mathcal{J}$ is a separating invariant for S_{pd}, and it is closed and semilinear if $\mathcal{I}$ is closed and semilinear.

Conversely, let $\mathcal{J}$ be a separating invariant for S_{pd}. Let

$$\mathcal{I} = \left\{ z \in \mathbb{R}^d : z^{\downarrow 1} \in \mathcal{J} \right\}.$$

We argue that $\mathcal{I}$ is a separating invariant for S_d. Clearly $x \in \mathcal{I}$ and $y \notin \mathcal{I}$. Let $z \in \mathcal{I}$ and $i \in [1, p]$, we show that $z \cdot M_i \in \mathcal{J}$, *i.e.* $(z \cdot M_i)^{\downarrow 1} \in \mathcal{I}$. We have

$$(z \cdot M_i)^{\downarrow 1} = z^{\downarrow 1} \cdot M_{\text{shift}}^{i-1} \cdot M \cdot M_{\text{shift}}^{d-i+1} \in \mathcal{J}$$

since $z^{\downarrow 1}$ and $\mathcal{I}$ is invariant under M and M_{shift}. Thus $\mathcal{I}$ is a separating invariant for S_d, and it is closed and semilinear if $\mathcal{J}$ is closed and semilinear.

Corollary 8 directly follows from Theorem 1 and Theorem 7 combined with Lemma 21.

5 Decidability proofs

5.1 Proof of Lemma 15

Let $\ell = (A, x, y)$ be an Orbit instance such that y is not reachable from x.

- The matrix A can be put in Jordan normal form through a change of basis using Lemma 14.
- Suppose A is not invertible, we distinguish two cases.

  - If for some Jordan block J associated with the eigenvalue 0, we have that y is not the zero vector, *i.e.*, $y_J \neq 0$, then $\mathcal{I} = \{x, Ax, \ldots, A^{d-1}x\} \cup \{z \in \mathbb{C}^d \mid z_J = 0\}$ is a semilinear invariant. Indeed, the Jordan block J is nilpotent, so for any point u and $n \geq d$, we have that $J^n u = 0$, so in particular $(A^n x)_J = 0$. Moreover, since by assumption y is not reachable, it is not one of $A^n x$ for $n < d$, and $y_J \neq 0$, so $y \notin \mathcal{I}$.
  - Otherwise, let J be a Jordan block associated with the eigenvalue 0, such that $y_J = 0$. Consider the Orbit instance $\ell' = (A_{J^c}, (A^d x)_{J^c}, y_{J^c})$. We claim that ℓ admits a semilinear invariant if, and only if, ℓ' does.

    Let $\mathcal{I}$ be a semilinear invariant for ℓ. Build $\mathcal{I}' = \{z \in \mathbb{C}^{J^c} \mid (z, 0) \in \mathcal{I}\}$. We argue that $\mathcal{I}'$ is a semilinear invariant for ℓ'. Indeed, $(A^d x)_{J^c} \in \mathcal{I}'$ since $A^d x \in \mathcal{I}$ and $(A^d x)_J = 0$, because the Jordan block J is nilpotent. The stability of $\mathcal{I}'$ under A_{J^c} is clear, and y_{J^c} is not in $\mathcal{I}'$ because $y_J = 0$, so if y_{J^c} would be in $\mathcal{I}'$ this would imply that y is in $\mathcal{I}$.

    Conversely, let $\mathcal{I}'$ be a semilinear invariant for ℓ', let $\mathcal{I} = \mathcal{I}' \times \mathbb{C}^J$, then $\{x, Ax, \ldots, A^{d-1}x\} \cup \mathcal{I}$ is a semilinear invariant for ℓ.

    We reduced the existence of semilinear invariants from ℓ to ℓ', removing one Jordan block J such that $y_J = 0$. Proceeding this way for each such Jordan block, we reduce to the case where the matrix is invertible.

- Suppose A contains a Jordan block J such that $x_{J,d(J)} = 0$. We distinguish two cases.
  - If for some Jordan block J we have $x_{J,d(J)} = 0$ and $y_{J,d(J)} \neq 0$, then the set $\mathcal{I} = \{z \in \mathbb{C}^d \mid z_{J,d(J)} = 0\}$ is a semilinear invariant for ℓ.
  - Otherwise, let J be a Jordan block such that $x_{J,d(J)} = y_{J,d(J)} = 0$. Write p for the dimension $(J, d(J))$. Consider the Orbit instance $\ell_p = (A_{p^c}, x_{p^c}, y_{p^c})$, we claim that ℓ admits a semilinear invariant if, and only if, ℓ_p does.

    Let $\mathcal{I}$ be a semilinear invariant for ℓ. Build $\mathcal{I}_p = \{z \in \mathbb{C}^{p^c} \mid (z, 0) \in \mathcal{I}\}$, then $\mathcal{I}_p$ is a semilinear invariant for ℓ_p. Conversely, let $\mathcal{I}_p$ be a semilinear invariant for ℓ_p, let $\mathcal{I} = \{z \in \mathbb{C}^d \mid z_p = 0 \text{ and } z_{p^c} \in \mathcal{I}_p\}$, then $\mathcal{I}$ is a semilinear invariant for ℓ.

    We reduced the existence of semilinear invariants from ℓ to ℓ_p, removing the last dimension in a Jordan block J such that $x_{J,d(J)} = 0$. Proceeding this way for each such Jordan block, we reduce to the case where there are no such Jordan blocks.

- Suppose A has a diagonal Jordan block J, that is, $d(J) = 1$, with eigenvalue λ with $\lambda^n = 1$. We set n minimal such that $\lambda^n = 1$ and distinguish two cases
  - If for every $k \leq n-1$, $y_J \neq \lambda^k x_J$, then the set $\mathcal{I} = \bigcup_{k=0}^{n-1} \{z \mid z_J = \lambda^k x_J\}$ is a semilinear invariant for ℓ.
  - Otherwise, let $k \leq n-1$ be such that $y_J = \lambda^k x_J$. We claim that there exists an invariant for ℓ if and only if there exists an invariant for $\ell' = (A^n_{J^c}, A^k_{J^c} x_{J^c}, y_{J^c})$. Let $\mathcal{I}'$ be an invariant for ℓ'. For $k' \in \{0, \ldots, n-1\}$, we put

    $$\mathcal{I}_{k'} = \{z \mid z_J = \lambda^{k+k'} x_J \text{ and } z_{J^c} \in A^{k'}_{J^c} \mathcal{I}'\},$$

    $\mathcal{I} = \{x, Ax, \ldots, A^{k-1}x\} \cup \bigcup_{k'=0}^{n-1} \mathcal{I}_{k'}$, and prove that the semilinear set $\mathcal{I}$ is an invariant for ℓ. It is clear that $x \in \mathcal{I}$. Moreover, y does not

  belong to $\mathcal{I}$: indeed, $y \notin \{x, Ax, \dots, A^{k-1}x\}$ and $y \notin \bigcup_{k'=1}^{n-1} \mathcal{I}_{k'}$ because $y_J = \lambda^k x_J \neq \lambda^{k+k'} x_J$ for any $k' \in \{1, \dots, n-1\}$ (we assume $x_J \neq 0$ thanks to a previous reduction), and $y \notin \mathcal{I}_0$ since $\mathcal{I}'$ is an invariant for ℓ'. Finally, $\mathcal{I}$ is stable for A since $A^k x \in \mathcal{I}_0$, $A\mathcal{I}_{k'} = \mathcal{I}_{k'+1}$ if $k < n-1$ and $A\mathcal{I}_{n-1} = A^n \mathcal{I}_0 \subseteq \mathcal{I}_0$ since $\lambda^n = 1$ and $A^n_{J^{\mathsf{c}}} \mathcal{I}' \subseteq \mathcal{I}'$.
  Conversely, let $\mathcal{I}$ be an invariant for ℓ. We let $\mathcal{I}'$ be the projection on J^{c} of $A^k \mathcal{I} \cap \{z \mid z_J = \lambda^k x_J\}$, and claim it is an invariant for ℓ'. Indeed, quite clearly $A^k_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}} \in \mathcal{I}'$ and $\mathcal{I}'$ is stable for $A^n_{J^{\mathsf{c}}}$. Now, if $y_{J^{\mathsf{c}}} \in \mathcal{I}'$ then it must be that $y \in \mathcal{I}$, a contradiction.

- Let J be a Jordan block of A with eigenvalue $\lambda < 1$ and such that $y_J = 0$. If there are infinitely many integers n such that $A^n_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}} = y_{J^{\mathsf{c}}}$, then $y \in \overline{\{A^n x, n \in \mathbb{N}\}}$, so there exists no closed invariant for ℓ. Otherwise, we let $n_0 \in \mathbb{N}$ be such that $y_{J^{\mathsf{c}}} \notin \{A^n_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}}, n \geq n_0\}$, and claim that ℓ is equivalent to $\ell' = (A_{J^{\mathsf{c}}}, A^{n_0}_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}}, y_{J^{\mathsf{c}}})$. Let $\mathcal{I}'$ be a semilinear invariant for ℓ'. Then $\mathcal{I} = \{x, Ax, \dots, A^{n_0-1}x\} \cup \{z \mid z_{J^{\mathsf{c}}} \in \mathcal{I}'\}$ is an invariant for ℓ. Conversely, let $\mathcal{I}$ be an invariant for ℓ. Let $\delta = \frac{1}{2} d(y, \mathcal{I}) > 0$, where the distance is defined according to the infinity norm on $\mathbb{C}^d$. Using Lemma 25 from section 5.3, we construct a semilinear $P \subseteq \mathbb{C}^J$ which is stable for A_J, contains $(A^n x)_J$ for some n, and is included in $B(0, \delta)$. Let $\mathcal{I}'$ be the projection of $\{z \mid z \in \mathcal{I} \text{ and } z_J \in P\}$ on J^{c}. Then $A^n_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}} \in \mathcal{I}'$ and $\mathcal{I}'$ is stable for $A_{J^{\mathsf{c}}}$. Assume that $y_{J^{\mathsf{c}}} \in \mathcal{I}'$, that is, there exists $\tilde{y} \in P$ such that $y_1 = (y_{J^{\mathsf{c}}}, \tilde{y}) \in \mathcal{I}$. Then $d(y, \mathcal{I}) \leq d(y, y_1) = ||\tilde{y}|| \leq \delta/2$ which is a contradiction, so $y_{J^{\mathsf{c}}} \notin \mathcal{I}'$. Finally, $\{A^{n_0}_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}}, A^{n_0+1}_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}}, \dots, A^{n-1}_{J^{\mathsf{c}}} x_{J^{\mathsf{c}}}\} \cup \mathcal{I}'$ is an invariant for ℓ' which concludes the proof.

5.2 Some eigenvalue has modulus greater than 1

We start with a simple lemma.

Lemma 22. *Let λ be a complex non-real number of modulus greater than* 1 *and x be a non-zero complex number. Then the sequence of polyhedra in $\mathbb{C}$ $\left(Conv\left(\left\{\lambda^i x \mid i \in \{0, \dots, n\}\right\}\right)\right)_{n \in \mathbb{N}}$ is strictly increasing and its limit is $\mathbb{C}$.*

Proof. To see that the sequence is strictly increasing, observe that for all n in $\mathbb{N}$, we have

$$\mathrm{Conv}\left(\left\{\lambda^i x \mid i \in \{0, \dots, n\}\right\}\right) \subseteq \overline{B}(0, |\lambda|^n \cdot |x|).$$

It follows that $\lambda^{n+1} x$ is not in $\mathrm{Conv}\left(\left\{\lambda^i x \mid i \in \{0, \dots, n\}\right\}\right)$.

We now prove that its limit is $\mathbb{C}$. We write $x = |x| e^{i\theta}$ and $\lambda = |\lambda| e^{i\alpha}$, with θ, α in $[0, 2\pi)$. Since λ is not a real number, α is not 0. Let n_0 in $\mathbb{N}$ such that $n_0 \alpha > 2\pi$. Observe that 0 is in $\mathrm{Conv}\left(\left\{\lambda^i x \mid i \in \{0, \dots, n_0\}\right\}\right)$.

We claim that for all $n \in \mathbb{N}$, we have

$$B(0, |\lambda|^n \cdot |x|) \subseteq \mathrm{Conv}\left(\left\{\lambda^i x \mid i \in \{0, \dots, n + n_0\}\right\}\right).$$

Let $z = |z| e^{i\beta}$ such that $|z| < |\lambda|^n \cdot |x|$. Let p in $\{0, \dots, n_0 - 1\}$ such that β is in $[\theta + (n+p)\alpha, \theta + (n+p+1)\alpha)$. Then z is in $\mathrm{Conv}\left(\left\{0, \lambda^{n+p} x, \lambda^{n+p+1} x\right\}\right)$.

The claim follows, since the union of the balls $B(0, |\lambda|^n \cdot |x|)$ for $n \in \mathbb{N}$ is $\mathbb{C}$.

Theorem 23. *Let $\ell = (A, x, y)$ be a normalized Orbit instance in Jordan normal form such that y is not reachable from x. If the matrix A has an eigenvalue whose modulus is greater than 1, then there exists a semilinear invariant for ℓ.*

On an intuitive level first: some coordinate of $(A^n x)_{n\in\mathbb{N}}$ diverges to infinity, so eventually gets larger in absolute value than the corresponding coordinate in y. This allows us to construct an invariant for ℓ by taking the first points and then all points having a large coordinate in the diverging dimension. For the invariant to be semilinear we consider the complement of the convex envelope of an initial segment of points.

Proof. Let J be a Jordan block of A with eigenvalue λ of modulus > 1. Since ℓ is non-trivial, we have $x_{J,d(J)} \neq 0$. We distinguish two cases.

- Suppose that λ is a real number.
  For all $n \in \mathbb{N}$, we have $(A^n x)_{J,d(J)} = \lambda^n x_{J,d(J)}$, so it diverges to infinity in modulus. It follows that there exists n_0 in $\mathbb{N}$ such that $|(A^{n_0}x)_{J,d(J)}| > 2\sqrt{2} \cdot |y_{J,d(J)}|$. Let

  $$\mathcal{I} = \left\{x, Ax, \ldots, A^{n_0-1}x\right\} \cup \left\{z \in \mathbb{C}^d \mid |\mathrm{Re}\left(z_{J,d}\right)| + |\mathrm{Im}\left(z_{J,d}\right)| \geq 2|y_{J,d(J)}|\right\} .$$

  We argue that $\mathcal{I}$ is a semilinear invariant for ℓ. The non-trivial point is that $\mathcal{I}$ is stable under J. First, $A^{n_0}x$ is in $\mathcal{I}$ because

  $$|\mathrm{Re}\left((A^{n_0}x)_{J,d(J)}\right)| + \mathrm{Im}\left((A^{n_0}x)_{J,d(J)}\right) \geq \frac{1}{\sqrt{2}} \cdot |(A^{n_0}x)_{J,d(J)}| > 2|y_{J,d(J)}|.$$

  Second, let $z \in \mathbb{C}^d$ such that $|\mathrm{Re}\left(z_{J,d(J)}\right)| + |\mathrm{Im}\left(z_{J,d(J)}\right)| \geq 2|y_d|$, we have that $(Az)_{J,d(J)} = \lambda z_{J,d(J)}$, so $|\mathrm{Re}\left((Az)_{J,d(J)}\right)| + |\mathrm{Im}\left((Az)_{J,d(J)}\right)| = |\lambda|(|\mathrm{Re}\left(z_{J,d(J)}\right)| + |\mathrm{Im}\left(z_{J,d(J)}\right)|) > 2|y_{J,d(J)}|$, implying that Az is in $\mathcal{I}$. Note that the previous equality holds because λ is a real number.
- Suppose that λ is not a real number.
  Consider the sequence $\left(\mathrm{Conv}\left(\left\{\lambda^i x_{J,d(J)} \mid i \in \{1, \ldots, n\}\right\}\right)\right)_{n\in\mathbb{N}}$ of polyhedra in $\mathbb{C}$. Thanks to Lemma 22, this sequence is strictly increasing and its limit is $\mathbb{C}$. Let n_0 in $\mathbb{N}$ such that $y_{J,d(J)}$ and $x_{J,d(J)}$ are both in the interior of $\mathrm{Conv}\left(\left\{\lambda^i x_{J,d(J)} \mid i \in \{1, \ldots, n_0\}\right\}\right)$. Let us denote this convex set by C, and let

  $$\mathcal{I} = \{x, Ax, \ldots, A^{n_0}x\} \cup \overline{\left\{z \in \mathbb{C}^d \mid z_{J,d(J)} \notin C\right\}}.$$

  We argue that $\mathcal{I}$ is a semilinear invariant for ℓ. The non-trivial point is that $\mathcal{I}$ is stable under A.
  We first need to prove that $A^{n_0+1}x$ is in $\mathcal{I}$. We have $(A^{n_0+1}x)_{J,d(J)} = \lambda^{n_0+1}x_{J,d(J)}$, which is not in

  $$\overline{\mathrm{Conv}\left(\left\{\lambda^i x_{J,d(J)} \mid i \in \{1, \ldots, n_0\}\right\}\right)},$$

  because this sequence of polyhedra is strictly increasing. Thus $A^{n_0+1}x$ is in $\mathcal{I}$.

Finally, let $z \in \mathbb{C}^d$ such that $z_{J,d(J)} \notin \overline{C}$, we show that Az is in $\mathcal{I}$. We have $(Az)_{J,d(J)} = \lambda z_{J,d(J)}$. Assume towards contradiction that $(Az)_{J,d(J)}$ is in C, so $\lambda z_{J,d(J)}$ is a convex combination of $\left\{\lambda^i x_{J,d(J)} \mid i \in \{1,\ldots,n_0\}\right\}$. This implies that $z_{J,d(J)}$ is a convex combination of $\left\{\lambda^{i-1} x_{J,d(J)} \mid i \in \{1,\ldots,n_0\}\right\}$. Since $x_{J,d(J)}$ is in C, this implies that $z_{J,d(J)}$ is in C, which is a contradiction. Thus Az is in $\mathcal{I}$, and $\mathcal{I}$ is a semilinear invariant for ℓ.

5.3 Some eigenvalue has modulus less than 1

We start with a simple lemma.

Lemma 24. *Let λ be a complex non-real number of modulus less than 1 and x be a non-zero complex number. Then the sequence $\left(Conv\left(\left\{\lambda^i x \mid i \in \{0,\ldots,n\}\right\}\right)\right)_{n\in\mathbb{N}}$ of polyhedra in $\mathbb{C}$ is ultimately constant, and its limit contains an open neighbourhood of 0.*

Proof. We write $x = |x|e^{i\theta}$ and $\lambda = |\lambda|e^{i\alpha}$, with θ, α in $[0, 2\pi)$. Since λ is not a real number, α is not 0. Let n_0 in $\mathbb{N}$ such that $n_0\alpha > 2\pi$. Observe that 0 is in $\mathrm{Conv}\left(\left\{\lambda^i x \mid i \in \{0,\ldots,n_0\}\right\}\right)$.

We claim that $B(0, |\lambda|^{n_0} \cdot |x|)$ is included in $\mathrm{Conv}\left(\left\{\lambda^i x \mid i \in \{0,\ldots,n_0\}\right\}\right)$. Let $z = |z|e^{i\beta}$ such that $|z| < |\lambda|^{n_0} \cdot |x|$. Let p in $\{0,\ldots,n_0-1\}$ such that β is in $[\theta + p\alpha, \theta + (p+1)\alpha)$. Then z is in $\mathrm{Conv}\left(\left\{0, \lambda^p x, \lambda^{p+1} x\right\}\right)$.

The claim follows, since for all $n > n_0$, we have that $\lambda^n x$ is in $B(0, |\lambda|^{n_0} \cdot |x|)$.

The following Lemma is the cornerstone for this section.

Lemma 25. *Let $\varepsilon > 0$ and $\lambda \in \mathbb{C}$ with $|\lambda| < 1$. There exists a semilinear set $\mathcal{I} \subseteq B(0,\varepsilon) \subseteq \mathbb{C}^d$ which is stable for $\mathcal{J}_d(\lambda)$, and contains $B(0,\varepsilon')$ for some $0 < \varepsilon' < \varepsilon$.*

Proof. We let J denote $\mathcal{J}_d(\lambda)$, and prove the Lemma by induction on d. We first treat the case where $\lambda \in \mathbb{R}$. Let

$$\mathcal{I} = \left\{z \in \mathbb{C}^d \mid \forall i, |\mathrm{Re}\,(z_i)\,| + |\mathrm{Im}\,(z_i)\,| \leq \varepsilon(1-|\lambda|)^i\right\} \subseteq B(0,\varepsilon).$$

Then $B(0, \varepsilon(1-|\lambda|)^d/2) \subseteq \mathcal{I}$. We show that $J\mathcal{I} \subseteq \mathcal{I}$. Let $z \in \mathcal{I}$. Then $(Jz)_d = \lambda z_d$, so $|\mathrm{Re}\,((Jz)_d)\,| + |\mathrm{Im}\,((Jz)_d)\,| \leq |\lambda|(|\mathrm{Re}\,(z_d)\,| + |\mathrm{Im}\,(z_d)\,|) \leq \varepsilon(1-|\lambda|)^d$. Now if $i < d$, $(Jz)_i = \lambda z_i + z_{i+1}$, so

$$\begin{aligned}|\mathrm{Re}\,((Jz)_i)\,| + |\mathrm{Im}\,((Jz)_i)\,| &= |\lambda \mathrm{Re}\,(z_i) + \mathrm{Re}\,(z_{i+1})\,| + |\lambda \mathrm{Im}\,(z_i) + \mathrm{Im}\,(z_{i+1})\,| \\ &\leq |\lambda|(|\mathrm{Re}\,(z_i)\,| + |\mathrm{Im}\,(z_i)\,|) + (|\mathrm{Re}\,(z_{i+1})\,| + |\mathrm{Im}\,(z_{i+1})\,|) \\ &\leq |\lambda|\varepsilon(1-|\lambda|)^i + \varepsilon(1-|\lambda|)^{i+1} = \varepsilon(1-|\lambda|)^i.\end{aligned}$$

Hence $\mathcal{I}$ is stable for J, which concludes this first case. We now assume that $\lambda \notin \mathbb{R}$. We start with the base case $d = 1$. Let $u \in \mathbb{C}$ of modulus ε, for instance $u = \varepsilon$. We let $\mathcal{I} = \mathrm{Conv}\left(\left\{\lambda^i u \mid i \in \{0,\ldots,p\}\right\}\right)$. Since extremal points of $\mathcal{I}$ are of the form $\lambda^i u$, of modulus $|\lambda|^i \varepsilon < \varepsilon$, it holds that $\mathcal{I} \subseteq B(0,\varepsilon)$.

Let $d > 1$, and assume the result known for smaller dimensions. We let u be a complex number of modulus $\varepsilon/2$, for instance, $u = \varepsilon/2 \in \mathbb{C}$. We let $\alpha = |\lambda|^p \varepsilon$ which is such that $\alpha < \varepsilon$ and $B(0, \alpha) \subseteq \text{Conv}\left(\left\{\lambda^i u \mid i \in \{0, \ldots, p\}\right\}\right)$ and put $\varepsilon' = \frac{\alpha}{2}(1 - |\lambda|)$. We let $\mathcal{I}'$ be a semilinear subset of $\mathbb{C}^{d-1}$ given by induction, stable for $\mathcal{J}_{d-1}(\lambda)$, and such that

$$B(0, \varepsilon'') \subseteq \mathcal{I}' \subseteq B(0, \varepsilon') \subseteq \mathbb{C}^{d-1},$$

for some $\varepsilon'' > 0$. In particular, $0 \in \pi_1(\mathcal{I}')$.

We consider the sequence $(C_j)_{j \in \mathbb{N}}$ of semilinear subsets of $\mathbb{C}$ given by $C_0 = \{u\}$ and for all j,

$$C_{j+1} = \{\lambda z + z', z \in C_j, z' \in \pi_1(\mathcal{I}')\}.$$

Let us know prove two facts about the sequence $(C_j)_j$.

- For all j, and $z \in C_j$, $|z| \leq |\lambda|^j \frac{\varepsilon}{2} + \varepsilon' \sum_{i=0}^{j-1} |\lambda|^i$, which we prove by induction. This is clear for $j = 0$, and if it holds for elements $z \in C_j$, an element $\lambda z + z' \in C_{j+1}$ with $z' \in \pi_1(\mathcal{I}')$ is such that

$$|\lambda z + z'| \leq |\lambda| \left(|\lambda|^j \frac{\varepsilon}{2} + \varepsilon' \sum_{i=0}^{j-1} |\lambda|^i \right) + \varepsilon' \leq |\lambda|^{j+1} \frac{\varepsilon}{2} + \varepsilon' \sum_{i=0}^{j} |\lambda|^i.$$

- There exists j_0 such that $C_{j_0} \subseteq B(0, \alpha) \subseteq \text{Conv}\left(\{C_0, \ldots C_{j_0 - 1}\}\right)$. Indeed, the sequence $|\lambda|^j \frac{\varepsilon}{2} + \varepsilon' \sum_{i=0}^{j-1} |\lambda|^i$ goes to $\frac{\varepsilon'}{1 - |\lambda|}$, so for large enough j, $C_j \subseteq B(0, \frac{2\varepsilon'}{1 - |\lambda|}) = B(0, \alpha)$. Now $0 \in \pi_1(\mathcal{I}')$, so by an easy induction, $\lambda^j u \in C_j$. Hence,

$$C_{j_0} \subseteq B(0, \alpha) \subseteq \text{Conv}\left(\{\lambda^j u, j \in \mathbb{N}\}\right) \subseteq \text{Conv}\left(\{C_j, j \in \mathbb{N}\}\right) \subseteq \text{Conv}\left(\{C_0, \ldots, C_{j_0 - 1}\}\right).$$

We now let

$$\mathcal{I} = \text{Conv}\left(\{C_0, \ldots, C_{j_0 - 1}\}\right) \times \mathcal{I}',$$

Then

- $\mathcal{I} \subseteq B(0, \frac{\varepsilon}{2} + \frac{\varepsilon'}{1 - |\lambda|}) \subseteq B(0, \frac{\varepsilon}{2} + \frac{\alpha}{2}) \subseteq B(0, \varepsilon)$.
- $B(0, \min(\alpha, \varepsilon'')) \subseteq \mathcal{I}$, and
- $\mathcal{I}$ is stable for J, because $J(C_j \times \mathcal{I}') \subseteq C_{j+1} \times \mathcal{I}'$.

This concludes the induction, and the proof of the Lemma.

We may now prove the following theorem.

Theorem 26. *Let $\ell = (x, A, y)$ be a normalized Orbit instance such that y is not reachable from x. If the matrix A has an eigenvalue whose modulus is smaller than 1, then there exists a semilinear invariant for ℓ.*

Proof. Let J be a Jordan block of A with eigenvalue λ such that $|\lambda| < 1$. Since ℓ is normalized, $y_J \neq 0$. Let $\varepsilon = |y_J|/2$. Using Lemma 25, we obtain $\varepsilon' > 0$ and a semilinear set $\mathcal{I} \subseteq \mathbb{C}^{d(J)}$ such that $J\mathcal{I} \subseteq \mathcal{I}$ and $B(0,\varepsilon') \subseteq \mathcal{I} \subseteq B(0,\varepsilon)$. Now $(A^n x)_J \to 0$, so there exists n_0 such that $(A^{n_0}x)_J \in B(0,\varepsilon') \subseteq \mathcal{I}$. Hence, it is easy to see that

$$\{x, Ax, \ldots, A^{n_0-1}x\} \cup \{z \in \mathbb{C}^d \mid z_J \in \mathcal{I}\}$$

is a semilinear invariant for ℓ.

5.4 Some non-diagonalisable eigenvalue is a root of unity

Theorem 27. *Let $\ell = (A, x, y)$ be a normalized Orbit instance. Assume that ℓ is a non-reach instance. If A contains a non-diagonal Jordan block J whose eigenvalue is a root of unity, then there exists a semilinear invariant for ℓ.*

Proof. Let J be a non-diagonal Jordan block of A with eigenvalue λ with $\lambda^m = 1$. We shall use divergence on the coordinate $(J, d(J)-1)$ to construct an invariant. Recall that $x_{J,d(J)} \neq 0$. For any $n \in \mathbb{N}$, we have $(A^n x)_{J,d(J)-1} = \lambda^n x_{J,d(J)-1} + n\lambda^{n-1} x_{J,d(J)}$, and $(A^n x)_{J,d(J)} = \lambda^n x_{J,d(J)}$. Hence,

$$\operatorname{Re}\left(\lambda (A^n x)_{J,d(J)-1}\overline{(A^n x)_{J,d(J)}}\right) = \operatorname{Re}\left(\lambda x_{J,d(J)-1} x_{J,d(J)}\right) + n|x_{J,d(J)}|^2,$$

which goes to infinity when n grows. Note that this condition is quadratic, but since $(A^n x)_{J,d(J)}$ takes only a finite number of values, we will be able to state it in a semilinear fashion. Let n_0 be such that $M = \operatorname{Re}\left(\lambda (A^{n_0} x)_{J,d(J)-1}\overline{(A^{n_0} x)_{J,d(J)}}\right) > \operatorname{Re}\left(\lambda y_{J,d(J)-1}\overline{y_{J,d(J)}}\right)$. Let

$$\mathcal{I} = \{x, Ax, \ldots, A^{n_0-1}x\} \cup \bigcup_{i=0}^{m-1} \mathcal{I}_i,$$

where

$$\mathcal{I}_i = \{z \in \mathbb{C}^d \mid z_{J,d(J)} = \lambda^i x_{J,d(J)} \text{ and } \operatorname{Re}\left(\lambda z_{J,d(J)-1}\overline{z_{J,d(J)}}\right) \geq M)\}.$$

It is clear that $x \in \mathcal{I}$ and $y \notin \mathcal{I}$. Each $\mathcal{I}_i$ is semilinear because the second condition is actually semilinear assuming $z_{J,d(J)} = \lambda^i x_{J,d(J)}$. Now if $z \in \mathcal{I}_i$, we obtain that $(Az)_{J,d(J)} = \lambda z_{J,d(J)} = \lambda^{i+1} x_{J,d(J)}$, and

$$\operatorname{Re}\left(\lambda (Az)_{J,d(J)-1}\overline{Az_{J,d(J)}}\right) = \operatorname{Re}\left(\lambda z_{J,d(J)-1}\overline{z_{J,d(J)}}\right) + |z_{J,d(J)}|^2 \geq M$$

so $Az \in \mathcal{I}_{i+1}$ if $i < m$, and $Az \in \mathcal{I}_0$ (since $\lambda^m = 1$) if $i = m$. Hence $\mathcal{I}$ is stable for A.

5.5 All eigenvalues have modulus 1 and are not roots of unity

We finally deal with the most involved case, namely, when all eigenvalues have modulus 1 and none are roots of unity. In this setting, we will be able to describe the *minimal semilinear inviariant* for A and x, that is, a semilinear invariant which is contained in any semilinear invariant. We say that two eigenvalues are *equivalent* if their quotient is a root of unity. Intuitively, the only nontrivial semilinear relations that invariants will be able to exploit are the ones that hold among equivalent blocks.

We now give a high-level overview for this section.

- The first case is when eigenvalues are pairwise non-equivalent. The aim is to show that in this setting, any semilinear invariant is trivial. This is the object of subsection 5.5.1
  - We first consider the diagonal case. This makes a crucial use of the Skolem-Mahler-Lech theorem.
  - We then extend to general (possibly non-diagonal) blocks by induction on the total dimension. This is the most technical part of the proof.
- We then deal with equivalent eigenvalues in subsection 5.5.2: we first treat the case where all equivalent eigenvalues are equal, and then show how to reduce to this case.

5.5.1 All eigenvalues are non-equivalent

The diagonal case

We will make use of the following powerful theorem about linear recurrence sequences. This result is due to Skolem [31], and more general versions were subsequently obtained by Mahler [23, 24] and Lech [22].

Theorem 28 (Skolem, Mahler, Lech). *Let $(u_n)_{n\in\mathbb{N}}$ be a real non-degenerate linear recurrence sequence, that is, $u_n = \sum_{i=1}^{d} v_i\lambda_i^n$, for some $v \in \mathbb{C}^d\setminus\{0\}$, where for any $i \neq j$, $\frac{\lambda_i}{\lambda_j} \notin \mathbb{U}$. Then $\{n \in \mathbb{N} \mid u_n = 0\}$ is finite.*

We write $A = \mathrm{Diag}(\lambda_1, \ldots, \lambda_d)$ for

$$A = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_d \end{bmatrix}.$$

Lemma 29. *Let $\lambda_1, \ldots, \lambda_d \in S^1$ and $A = Diag(\lambda_1, \ldots, \lambda_d)$. Assume that:*

- *for all i, we have $\lambda_i \notin \mathbb{U}$, and*
- *for all i, j such that $i \neq j$, we have $\frac{\lambda_i}{\lambda_j} \notin \mathbb{U}$.*

Let $\mathcal{I}$ be a non-empty closed semilinear set stable under A, which moreover contains a point $x \in \mathcal{I}$ such that for all coordinate i, $x_i \neq 0$. Then $\mathcal{I} = \mathbb{C}^d$.

Proof. Let $\mathcal{I}$ be such a semilinear set, we show a few facts:

(i) $\mathcal{I}$ must have even dimension over $\mathbb{R}$,
(ii) $\mathcal{I}$ must have dimension $> 2d-2$ over $\mathbb{R}$ (hence, $\mathcal{I}$ has full dimension thanks to (i)),
(iii) $\partial\mathcal{I}$ is stable under A,
(iv) if it is non-empty (that is, if $\mathcal{I} \neq \mathbb{C}^d$), $\partial\mathcal{I}$ contains a point which is nonzero on each coordinate.

This implies the desired result: if towards contradiction we would have that $\mathcal{I} \neq \mathbb{C}^d$, then $\partial\mathcal{I}$ would be a non-empty closed semilinear set stable under A thanks to (iii), it would contain a point which is nonzero on each coordinate thanks to (iv), but yet it cannot have full dimension. We now prove the four claims.

(i) Let $s = \dim_{\mathbb{R}}(\mathcal{I})$. Then $\mathcal{I}$ is contained into the union of finitely many affine subspaces of dimension s, write

$$\mathcal{I} \subseteq \bigcup_{i=1}^{p} F_i,$$

where $F_i \subseteq \mathbb{C}^d \simeq \mathbb{R}^{2d}$ is a real affine space of dimension s, of direction $F_i - F_i = E_i \subseteq \mathbb{R}^{2d}$. We first show that for some i, E_i must be stable for some power of A (seen as a transformation of $\mathbb{R}^{2d}$), and then that this implies that s is even.
Since $\dim_{\mathbb{R}}(\mathcal{I}) \geq s$, there must be $\tilde{x} \in \mathcal{I}$ and $\varepsilon > 0$ such that

$$B(\tilde{x}, \varepsilon) \cap \mathcal{I} = B(\tilde{x}, \varepsilon) \cap F_i$$

for some i. Then for all n, $A^n(B(\tilde{x}, \varepsilon) \cap F_i) = B(A^n\tilde{x}, \varepsilon) \cap A^n F_i \subseteq \mathcal{I}$, and has dimension s over $\mathbb{R}$, hence there exists i_n such that $B(A^n\tilde{x}, \varepsilon) \cap \mathcal{I} = B(A^n\tilde{x}, \varepsilon) \cap F_{i_n}$. Now let $n_1 < n_2$ be such that $i_{n_1} = i_{n_2} = i$, let $n = n_2 - n_1$ and let $x = A^{n_1}\tilde{x}$. We show that E_i is stable under A^n.
Let $e \in E_i$, and let $\tilde{e} = \varepsilon \frac{e}{2||e||}$. Then $x + \tilde{e} \in B(x, \varepsilon) \cap F_i \subseteq \mathcal{I}$ so $A^n(x + \tilde{e}) = A^n x + A^n \tilde{e} \in B(A^n x, \varepsilon) \cap \mathcal{I} \subseteq F_i$ so $A^n \tilde{e} = A^n x + A^n \tilde{e} - A^n x \in F_i - F_i = E_i$ and since E_i is $\mathbb{R}$-linear, $A^n e \in E_i$.
Now since the λ_i's are not roots of 1, A^n, when seen as a transformation of R^{2d}, is the product of d diagonal irrationnal rotations of $\mathbb{R}^2$. Such a map only stabilizes linear spaces of even dimensions, hence $s = \dim_{\mathbb{R}}(E_i)$ is even.

(ii) Assume for contradiction that $\dim_{\mathbb{R}}(\mathcal{I}) \leq 2d-2$. Let $x \in \mathcal{I}$ be a point with $x_i \neq 0$ for all $i \in \{1, \ldots, d\}$. Now $\mathcal{I} \subseteq \bigcup_{i=1}^{p} F_i$, where the F_i's are affine spaces of real dimension $2d-2$, that is, spaces of the form

$$F_i = \{z \in \mathbb{C}^d \mid \sum_{i=1}^{d} u_i z_i = a\},$$

for some nonzero $u \in \mathbb{C}^d$ and some $a \in \mathbb{C}$. Consider the orbit $\mathcal{O} = \{A^n x, n \in \mathbb{N}\}$ of x. There must be i such that $F_i \cap \mathcal{O}$ is infinite, hence there are infinitely many $n \in \mathbb{N}$ such that

$$\sum_{i=1}^{d} \lambda_i^n u_i x_i = a,$$

which contradicts Theorem 28 applied to eigenvalues $\lambda_1, \ldots, \lambda_d, 1$, since $u \neq 0$ implies $(u_i x_i)_{i \in \{1,\ldots,d\}} \neq 0$.

- *(iii)* We argue that $\mathbb{C}^d \setminus \mathcal{I}$ is stable under A, which together with the fact that $\mathcal{I}$ is stable under A implies that $\partial \mathcal{I}$ is stable under A. Equivalently we show that $\mathcal{I}$ is stable under A^{-1}: let x in $\mathcal{I}$, we prove that $A^{-1}x$ is in $\mathcal{I}$. Let
$$L_A = \left\{ v \in \mathbb{Z}^d \mid \lambda_1^{v_1} \cdots \lambda_d^{v_d} = 1 \right\}$$
be the set of all multiplicative relations holding among $\lambda_1, \ldots, \lambda_d$. Notice that L_A is an additive subgroup of $\mathbb{Z}^d$. Consider the set of diagonal $d \times d$ matrices
$$T_A = \left\{ \mathrm{Diag}(\mu_1, \ldots, \mu_d) \mid \mu \in S^d \text{ and } \forall v \in L_A \, (\mu_1^{v_1} \cdots \mu_d^{v_d} = 1) \right\}$$
whose diagonal entries satisfy the multiplicative relations in L_A. Using Kronecker's Theorem on inhomogeneous simultaneous Diophantine approximation [5], it is shown in [29, Proposition 3.5] that $\{A^n : n \in \mathbb{N}\}$ is a dense subset of T_A. This immediately gives
$$\overline{\{A^n x \mid n \in \mathbb{N}\}} = \{Mx \mid M \in T_A\} \ .$$
Since x is in $\mathcal{I}$ and $\mathcal{I}$ is stable under A, we have that $\overline{\{A^n x \mid n \in \mathbb{N}\}} \subseteq \overline{\mathcal{I}} = \mathcal{I}$. Observe furthermore that $A^{-1} = \mathrm{Diag}(\lambda_1^{-1}, \ldots, \lambda_d^{-1})$ is in T_A, so thanks to the previous equality $A^{-1}x$ is in $\mathcal{I}$.

- *(iv)* Let $\mathcal{Q} = \bigcup_{i=1}^{d} \mathbb{C}^{i-1} \times \{0\} \times \mathbb{C}^{d-i}$ be the set of points with at least one zero coordinate. Assume for contradiction that $\partial \mathcal{I} \subseteq \mathcal{Q}$. Let $x \in \mathcal{I} \setminus \mathcal{Q}$ and $y \in \mathcal{I}^c \setminus \mathcal{Q}$, which is non-empty because $\mathcal{I}^c$ is a nonempty open subset of $\mathbb{C}^d$ whereas $\mathcal{Q}$ has empty interior. Now $\mathbb{C}^d \setminus \mathcal{Q}$ is path connected, so there exists a path from x to y which avoids $\mathcal{Q} \supseteq \partial \mathcal{I}$, a contradiction.

Although $\forall i, x_i \neq 0$ holds in a normalized instance, we shall need a slightly stronger result which is a consequence of the previous Lemma.

Theorem 30. *Let $A = Diag(\lambda_1, \ldots \lambda_d)$ with $\lambda_i \notin \mathbb{U}$ and for $i \neq j$, $\frac{\lambda_i}{\lambda_j} \notin \mathbb{U}$. Let $\mathcal{I} \subseteq \mathbb{C}^d$ be a closed semilinear set such that $A\mathcal{I} \subseteq \mathcal{I}$. Then $\mathcal{I}$ is a union of sets of the form*

$$\prod_{i=1}^{d} \varepsilon_i,$$

where $\varepsilon_i \in \{\{0\}, \mathbb{C}\}$.

Proof. We show that for any $x \in \mathcal{I}$, $\mathcal{I}$ must contain $\prod_i \varepsilon_i$, with $\varepsilon_i = \begin{cases} \{0\} \text{ if } x_i = 0 \\ \mathbb{C} \text{ otherwise} \end{cases}$, which implies the wanted result. This is an easy application of the previous Lemma to the projection of $\mathcal{I} \cap \prod_i \varepsilon_i$ on coordinates $\{i \mid x_i \neq 0\}$.

General case

We now work with a general (not necessarily diagonal) matrix A, whose eignvenvalues are not roots of unity and pairwise non equivalent. The following theorem is proved by induction on $d = \sum d_i$. We write $\mathcal{J}$ for the set of jordan blocks of A, and $s = |\mathcal{J}|$.

Theorem 31. *Semilinear invariants for A are unions of sets of the form*

$$\prod_{J \in \mathcal{J}} \mathbb{C}^{p_J} \times \{0\}^{d(J)-p_J},$$

where for each J, p_J is an integer in $\{0, \ldots, d(J)\}$.

Recall that if $S \subseteq \{(J,i), J \in \mathcal{J}, i \leq d(J)\}$ is a subset of dimensions, $\pi_S : \mathbb{C}^d \to \mathbb{C}^S$ denotes the projection on the coordinates in S. We let last $= \{(J, d(J)), J \in \mathcal{J}\}$ be the set of last coordinates of each block, and for each J, we let $P_J = \pi^{-1}_{\{(J,d(J))\}}(\{0\}) \subseteq \mathbb{C}^d$. Note that any set of the form $\prod_J \mathbb{C}^{p_J} \times \{0\}^{d(J)-p_J}$ which is not $\mathbb{C}^d$, is included in $\cup_J P_J$.

The case $d = 1$ is proved in section 5.5.1.

We start the induction with an intermediate result.

Lemma 32. *A semilinear invariant for A is either a union of sets of the form $\prod_{J \in \mathcal{J}} \mathbb{C}^{p_J} \times \{0\}^{d(J)-p_J}$, or contains $\pi^{-1}_{last}(\{0\}) = \prod_J \mathbb{C}^{d(J)-1} \times \{0\} = \mathcal{Q}$.*

Proof. Let $\mathcal{I}$ be a semilinear invariant for A. Consider $\mathcal{I}' = \pi_{\text{last}}(\mathcal{I}) \subseteq \mathbb{C}^s$. If $S' \subseteq \mathcal{J}$, we let $\pi'_{S'} : \mathbb{C}^s \to \mathbb{C}^{S'}$ denote the projection on the coordinates of $\mathbb{C}^s$ corresponding to last coordinates of blocks from S'. Just like previously, let $P'_J = {\pi'}^{-1}_J(\{0\}) \subseteq \mathbb{C}^s$. Since $\mathcal{I}'$ is stable for $\text{Diag}(\lambda_1, \ldots, \lambda_s)$, it must be that $\mathcal{I}'$ is either $\mathbb{C}^s$, or $\mathcal{I}' \subseteq \cup P'_J$, by Theorem 30. We reduce to the former case.

Indeed, if $\mathcal{I}' \subseteq \cup P'_J$, we let $\mathcal{I}_J = \pi^{-1}_{\text{last}}(P'_J)$, so that $\mathcal{I} = \cup \mathcal{I}_J$. Now, $\mathcal{I}_J \subseteq P_J$, so $\pi_{\{(J,d(J))\}^c}(\mathcal{I}_J)$ is stable for the matrix A' obtained from A just by diminishing the dimension of block J by 1. By induction, $\pi_{\{(J,d(J))\}^c}(\mathcal{I}_J)$ is a union of sets of the form $\prod_{J' \in \mathcal{J}'} \mathbb{C}^{p_{J'}} \times \{0\}^{d(J')-p_{J'}}$ (where $\mathcal{J}'$ is the set of Jordan blocks of A'), so $\mathcal{I}_J$ has the wanted form, and so does $\mathcal{I} = \cup I_J$.

Hence we assume that $\mathcal{I}' = \mathbb{C}^s$. We aim to show that $\mathcal{I} \supseteq \mathcal{Q}$, or equivalentely, $\pi_{\text{last}^c}(\mathcal{I} \cap \mathcal{Q}) = \mathbb{C}^{d-s}$. By induction, since it is stable for the matrix obtained from A by diminishing the dimension of each block by 1, we know that either $\pi_{\text{last}^c}(\mathcal{I} \cap \mathcal{Q}) = \mathbb{C}^{d-s}$, or $\pi_{\text{last}^c}(\mathcal{I} \cap \mathcal{Q}) \subseteq \cup_J \pi^{-1}_{\{(J,d(J)-1)\}}(\{0\})$. We assume the latter towards contradiction. In plain English, any $z \in \mathcal{I}$ that is 0 on the last coordinate of each block (that is, $z \in \mathcal{I} \cap \mathcal{Q}$) must have one of its prior coordinates (that is, $(J, d(J)-1)$ for some J) which is zero. We will now project on only the last two coordinates of each block. Formally, we let

$$\text{last-two} = \bigcup_{\substack{J\in\mathcal{J}\\ d(J)\geq 2}} \{(J, d(J)-1), (J, d_J)\} \cup \bigcup_{\substack{J\in\mathcal{J}\\ d(J)=1}} \{(J, 1)\},$$

and consider $\mathcal{I}'' = \pi_{\text{last-two}}(\mathcal{I})$. Then $\mathcal{I}''$ is stable for A'', the matrix obtained from A by reducing the size of each block of size ≥ 3 to 2. We let $\mathcal{J}''$ denote the set of Jordan blocks of A''. In particular, any $J'' \in \mathcal{J}''$ is such that $d(J'') \in \{1, 2\}$.

For each $J'' \in \mathcal{J}''$, we let $(z^{(n)}_{J'',d(J'')})_{n\in\mathbb{N}}$ be a decreasing sequence of complex numbers that goes to 0, and such that for any given n, the moduli of the $z^{(n)}_{J'',d(J'')}$ are all equal. Since $\mathcal{I}' = \mathbb{C}^s$, for all $n \in \mathbb{N}$ and each J'' such that $d(J'') = 2$ there exists $z^{(n)}_{J'',1}$ such that $z^{(n)} \in \mathcal{I}''$. By Lemma 4, we may pick these values such that $z^{(n)}$ is bounded. Up to extracing a subsequence, we assume without loss of generality that $z^{(n)}$ converges, to, say, $z \in \mathcal{I}''$. Since $z_{J'',d(J'')} = 0$ for all $J'' \in \mathcal{J}''$, $z \in \pi_{\text{last-two}}(\mathcal{I} \cap \mathcal{Q})$, so there must exist J''_0 with $d(J''_0) = 2$ such that $z_{J''_0,1} = 0$. We let λ_0 be the eigenvalue of block J''_0. We put $\delta = \min\Big(1, \min_{\{J''|d(J'')=2 \text{ and } z_{J'',1}\neq 0\}}\{|z_{J'',1}|\}\Big) > 0$. We let n be large enough so $||z^{(n)} - z|| \leq \delta/4$. Consider $({A''}^k z^{(n)})_{J''_0,1} = \lambda_0^n(z^{(n)}_{J''_0,1} + k\lambda_0^{-1} z^{(n)}_{J''_0,2})$. Let $k(n) = \left\lceil \frac{\delta}{2|z^{(n)}_{J''_0,2}|} \right\rceil$. Note that $k(n)$ does not depend on the choice of J''_0 since the $z^{(n)}_{J'',d(J'')}$ all have the same moduli. Then

$$\begin{aligned}\delta/4 = \delta/2 - \delta/4 \leq k(n)|z^{(n)}_{J''_0,2}| - |z^{(n)}_{J''_0,1}| \leq |({A''}^{k(n)} z^{(n)})_{J''_0,1}| \\ \leq |z^{(n)}_{J''_0,1}| + k(n)|z^{(n)}_{J''_0,2}| \leq \delta/4 + (\frac{\delta}{2|z^{(n)}_{J''_0,2}|} + 1)|z^{(n)}_{J''_0,2}| \leq \delta.\end{aligned}$$

Likewise, we may bound away from zero (which is the reason motivating the choice of δ), and also from above, the moduli of $({A''}^{k(n)} z^{(n)})_{J''_1,1}$ when J''_1 is such that $z_{J''_1,1} \neq 0$. More precisely,

$$\begin{aligned}\delta/4 = \delta - (\delta/4 + \delta/2) \leq |z_{J''_1,1}| - |z^{(n)}_{J''_1,1} - z_{J''_1,1} + k(n)\lambda^{-1} z^{(n)}_{J''_1,2}| \leq |({A''}^{k(n)} z)_{J''_1,1}| \\ \leq |z^{(n)}_{J''_1,1} - z_{J''_1,1}| + |z_{J''_1,1}| + k(n)|z^{(n)}_{J''_1,2}| \leq \delta/4 + |z_{J''_1,1}| + \delta/2 + \delta/4 \leq |z_{J''_1,1}| + \delta.\end{aligned}$$

Now, $\mathcal{I}''$ being stable for A'', the sequence $({A''}^{k(n)} z^n)_n$ has its elements in $\mathcal{I}''$, and ultimately lies in the compact

$$K = \{u \mid \forall J'', u_{J'',d(J'')} \leq \delta/4 \text{ and } \forall J'' \text{ such that } d(J'') = 2, \delta/4 \leq |u_{J'',1}| \leq |z_{J'',1}| + \delta\}.$$

We may then extract a converging subsequence in K, with its limit in $\mathcal{I}''$ such that the last coordinate of each block is zero whereas the previous one is nonzero, a contradiction. This concludes the proof of the Lemma.

With Lemma 32 in hands, we now move on to the proof of Theorem 31.

Proof. Let us assume for contradiction that $\mathcal{I}$ is not in the form of the statement of the Theorem. In particular, $\mathcal{I} \neq \mathbb{C}^s$. By Lemma 32, $\mathcal{Q} \subseteq \mathcal{I}$. The set $\mathcal{I}$ is a finite union of closed polyhedra, write $\mathcal{I} = \bigcup_{\mathcal{P} \in P} \mathcal{P}$. Each polyhedron $\mathcal{P}$ is a finite intersection of closed half-spaces, write $\mathcal{P} = \bigcap_{\mathcal{H} \in H_{\mathcal{P}}} \mathcal{H}$. Let $H = \bigcup_{\mathcal{P} \in P} \mathcal{H}_{\mathcal{P}}$.

We start with a restriction: we may restrict to the case where there is a polyhedron $\mathcal{P}_0 \in P$ such that $\mathcal{P}_0 \cap \mathcal{Q}$ has dimension (over $\mathbb{R}$) $2(d-s)$, and $\mathcal{P}_0$ is not included in $\mathcal{Q}$.

Let P_{full} denote the set of polyhedra $\mathcal{P}$ in P such that $\mathcal{P} \cap \mathcal{Q}$ has dimension $2(d-s)$. Since $\mathcal{Q} \subseteq \mathcal{I}$, $P_{full} \neq \emptyset$. Assume that for each polyhedron $\mathcal{P}$ of P_{full} we have $\mathcal{P} \subseteq \mathcal{Q}$. Let

$$\mathcal{I}' = \overline{\mathcal{I} \setminus \mathcal{Q}} \subseteq \bigcup_{\mathcal{P} \notin P_{full}} \mathcal{P}.$$

Since $\mathcal{I}' \cap \mathcal{Q}$ has dimension at most $2(d-s) - 1 < \dim_{\mathbb{R}}(\mathcal{Q})$, it may not be the case that $\mathcal{Q} \subseteq \mathcal{I}'$. Now $\mathcal{Q}^{\mathsf{c}}$ is stable for A, so so is $\mathcal{I}'$. Hence $\mathcal{I}'$ is, by Lemma 32 in the form of the Theorem. Finally, $I = \mathbb{Q} \cup \mathcal{I}''$ is in the wanted form. Hence, we now assume the existence of $\mathcal{P}_0 \in P_{full}$ which is not contained in $\mathcal{Q}$.

Let $H_{general}$ be the family of half-spaces in H which are not of the form $\pi_{\text{last}}^{-1}(\mathcal{H}')$ where $\mathcal{H}'$ is a half-space of $\mathbb{C}^s$ with $0 \in \partial\mathcal{H}'$. Equivalentely, half-spaces in $H_{general}$ are those which do not contain $\mathcal{Q}$ in their border. Now if $\mathcal{H} \in H_{general}$ then $\partial\mathcal{H} \cap \mathcal{Q}$ has dimension $< 2(d-s)$.

It follows that the countable union $\bigcup_{\mathcal{H} \in H_{general}} \bigcup_{k \in \mathbb{N}} A^{-k}\partial\mathcal{H} \cap \mathcal{Q}$ has dimension $< 2(d-s)$, so it may not cover $\mathcal{P}_0 \cap \mathcal{Q}$. Let $z \in \mathcal{P}_0 \cap \mathcal{Q}$ be out of this union.

Let k in $\mathbb{N}$. We choose $\varepsilon_k > 0$ such that for each $\mathcal{H} \in H$, the set $B(A^k z, \varepsilon_k) \cap \mathcal{H}$ is either empty, the whole ball $B(A^k z, \varepsilon_k)$, or a half-ball of the form $B(A^k z, \varepsilon_k) \cap \pi_{\text{last}}^{-1}(\mathcal{H}')$, where $\mathcal{H}'$ is a half-space of $\mathbb{C}^s$ such that $0 \in \partial\mathcal{H}'$. This is achieved by the following case disctinction:

- Either $A^k z$ is in $\mathcal{H}^{\text{o}}$, then there exists $\varepsilon_k > 0$ such that $B(A^k z, \varepsilon_k) \cap \mathcal{H} = B(A^k z, \varepsilon_k)$.
- Or $A^k z$ is in $\partial\mathcal{H}$. Recall that by construction $A^k z$ is not in $\partial\mathcal{H}$ for $\mathcal{H}$ in $H_{general}$, so $\mathcal{H} \notin H_{general}$ and we are in the third case.
- Or $A^k z$ is not in $\mathcal{H}$, in which case there exsits $\varepsilon_k > 0$ such that $B(A^k z, \varepsilon_k) \cap \mathcal{H} = \varnothing$.

Without loss of generality, we pick $(\varepsilon_k)_k$ to be decreasing.

It follows that for a polyhedron $\mathcal{P} \in P$, its trace on $B(A^k z, \varepsilon_k)$ is either empty or of the form

$$B(A^k z, \varepsilon_k) \cap \mathcal{P} = B(A^k z, \varepsilon_k) \cap \pi_{last}^{-1}\left(\bigcap_{\mathcal{H} \in H_{\mathcal{P}}^k} \mathcal{H}\right)$$

where $H_{\mathcal{P}}^k$ is a finite set of closed half-spaces $\mathcal{H}$ of $\mathbb{C}^s$ such that $0 \in \partial\mathcal{H}$. For $\mathcal{P} \in P$, let $C_{\mathcal{P},k} = \bigcap_{\mathcal{H} \in H_{\mathcal{P}}^k} \mathcal{H}$ and $C_k = \bigcup_{\mathcal{P} \in P} C_{\mathcal{P},k}$. By construction, forall

$k \in \mathbb{N}$,

$$B(A^k z, \varepsilon_k) \cap \mathcal{I} = B(A^k z, \varepsilon_k) \cap \pi_{\mathrm{last}}^{-1}(C_k).$$

We make three claims.

- C_k has full dimension (over $\mathbb{R}$) $2s$. Indeed, since z avoids $\bigcup_{\mathcal{H} \in H_{general}} \partial\mathcal{H}$, and $\dim_{\mathbb{R}}(\mathcal{P}_0 \cap Q) = 2s$, C_0 has full dimension. Since $\mathrm{Diag}\{\lambda_1, \ldots, \lambda_s\} C_k \subseteq C_{k+1}$, the claim follows by a easy induction.
- C_k is not all of $\mathbb{C}^s$. For this, let us consider $\overline{\mathcal{I}^{\mathsf{c}}}$, a closed semilinear set which is stable for A^{-1}. Under an appropriate diagonal change of basis, which, in particular, stabilizes any set of of form $\prod_{J \in \mathcal{J}} \mathbb{C}^{p_J} \times \{0\}^{d(J)-p_J}$, A^{-1} rewrites as $\mathrm{Diag}(\mathcal{J}_{d(J)}(\lambda_J^{-1}), J \in \mathcal{J})$. Hence Lemma 32 applies to $\overline{\mathcal{I}^{\mathsf{c}}}$. Since $\mathcal{I} \neq \mathbb{C}^s$, $\mathcal{I}^{\mathsf{c}}$ is nonempty, and since it is an open set, it must be fully dimensional. Hence, either $\overline{\mathcal{I}^{\mathsf{c}}} \subseteq \mathcal{Q}$, that is, each point of Q (in particular, $A^k z$) has arbitrary close points that are not in $\mathcal{I}$, which implies the claim.
- There are finitely many different sets C_k for k in $\mathbb{N}$. Indeed, C_k is determined by finitely many queries, namely whether $A^k z$ is in $\mathcal{H}^{\mathrm{o}}, \partial\mathcal{H}$ or not in $\mathcal{H}$, for each $\mathcal{H}$ in H. Note that on the other hand, ε_k does depend on k, and may take arbitrarily small values if $A^k z$ gets arbitrarily close to some $\mathcal{H}$ in H when k ranges in $\mathbb{N}$.

As previously stated, $\{(\lambda_1^k, \ldots, \lambda_s^k), k \in \mathbb{N}\}$ is dense in $\{(\lambda_1^t, \ldots, \lambda_s^t), t \in \mathbb{R}\} \subseteq T_A$. Hence, there exists an increasing sequence $\varphi : \mathbb{N} \to \mathbb{N}$ and $\varepsilon_k/2 \leq \mu_k \leq \varepsilon_k$ such that forall k, $(\lambda_1^{\varphi(k)}, \ldots, \lambda_s^{\varphi(k)}) = (\lambda_1^{\mu_k}, \ldots, \lambda_s^{\mu_k})$. Let C be such that $C = C_{\varphi(k)}$ for infinitely many k. Combining the diagonal case from section 5.5.1, the fact that C has full dimension, and that C is not $\mathbb{C}^s$, we know that C cannot stabilize $\mathrm{Diag}(\lambda_1, \ldots, \lambda_s)$. In particular, there is $\tilde{u} \in C$ such that $\mathrm{Diag}(\lambda_1, \ldots, \lambda_s)\tilde{u} \notin C$. Let $t_0 = \inf\{t \leq 1, \mathrm{Diag}(\lambda_1^t, \ldots, \lambda_s^t)\tilde{u} \notin C\} \geq 0$, and $u = \mathrm{Diag}(\lambda_1^{t_0}, \ldots, \lambda_s^{t_0})\tilde{u} \in C$, since C is closed. Note that for any small enough $\varepsilon > 0, \mathrm{Diag}(\lambda_1^{\varepsilon}, \ldots, \lambda_s^{\varepsilon})u \notin C$. We let $N \in \mathbb{N}$ be such that for $n \geq N$, ε_n is small enough in this sense, and N' be such that $\varphi(N') - \varphi(0) \geq N$. Recall that C is defined using half-spaces which contain 0 in their border, hence it is invariant under multiplication by positive reals (a cone). Hence we may assume that $||u|| \leq 2^{-\varphi(N')}\varepsilon_{\varphi(N')}$.

We may finaly give the last construction. Let $v \in B(A^{\varphi(0)}z, 2^{-\varphi(N')}\varepsilon_{\varphi(N')}) \cap \pi_{last}^{-1}(\{u\}) \subseteq B(A^{\varphi(0)}z, \varepsilon_{\varphi(0)}) \cap \pi_{\mathrm{last}}^{-1}(C) \subseteq \mathcal{I}$. We argue that $A^{\varphi(N')-\varphi(0)}v \in B(A^{\varphi(N')}z, \varepsilon_{\varphi(N')})$. Indeed, A is 2-lipschitzian, so $A^{\varphi(N')-\varphi(0)}$ is $2^{\varphi(N')}$-lipschitzian, so

$$||A^{\varphi(N')-\varphi(0)}v - A^{\varphi(N')}z|| \leq 2^{\varphi(N')}||v - A^{\varphi(0)}z|| \leq \varepsilon_{\varphi(N')}.$$

Hence, $A^{\varphi(N')-\varphi(0)}v \in B(A^{\varphi(N')}z, \varepsilon_{\varphi(N')}) \cap \mathcal{I} = B(A^{\varphi(N')}z, \varepsilon_{\varphi(N')}) \cap \pi_{\mathrm{last}}^{-1}(C)$, but

$$\pi_{\mathrm{last}}(A^{\varphi(N')-\varphi(0)}v) = \mathrm{Diag}(\lambda_1^{\varphi(N')}, \ldots, \lambda_s^{\varphi(N')})u = \mathrm{Diag}(\lambda_1^{\mu_{N'}}, \ldots, \lambda_s^{\mu_{N'}}),$$

and since $\mu_{N'} \leq \varepsilon_{N'} \leq \varepsilon_N$, we obtain that $\pi_{\mathrm{last}}(A^{\varphi(N')-\varphi(0)}v) \notin C$, a contradiction.

Note that Theorem 31 gives a minimal semilinear invariant for A which contains a given $x \in \mathbb{C}^d$, namely,

$$\mathcal{I} = \prod_{J \in \mathcal{J}} \mathbb{C}^{p_J} \times \{0\}^{d(J)-p_J},$$

where $p_J = \max\{i \leq d(J) \mid x_{J,i} \neq 0\}$. In particular, if the instance is reduced, $x_{J,d(J)} \neq 0$ so the minimal semilinear invariant is $\mathbb{C}^d$.

5.5.2 Some eigenvalues may be equivalent We will show that this case reduces to the previous one. We first deal with the case where all equivalent eigenvalues are in fact equal, which we then extend to the general case. Let us start with a Lemma.

Lemma 33. *Let*

$$A = \begin{bmatrix} A'' & & \\ & \mathcal{J}_{d_1}(\lambda) & \\ & & \mathcal{J}_{d_2}(\lambda) \end{bmatrix},$$

and $x = (x'', x_1, x_2) \in \mathbb{C}^s$ *with* $s = s'' + d_1 + d_2$, s'' *being the dimension of* A'' *(hence* s *is the dimension of* A*). The* $i-th$ *coordinate of* x *in the* $\mathcal{J}_{d_1}(\lambda)$ *block (resp. in the* $\mathcal{J}_{d_2}(\lambda)$ *block) is denoted* $x_{1,i}$ *(resp.* $x_{2,i}$*). We assume that* $x_{1,d_1} \neq 0$ *and let*

$$A' = \begin{bmatrix} A'' & & \\ & J_{d_1}(\lambda) & \\ & \frac{x_{2,d_2}}{x_{1,d_1}} E_{d_2-1,d_1} & J_{d_2-1}(\lambda) \end{bmatrix},$$

of size $s' = s - 1$, *where* E_{d_2-1,d_1} *denotes the matrix with* $d_2 - 1$ *rows and* d_1 *columns with a single 1 in the bottom right corner. We let* $x' = (x'', x_1, x_2')$ *be given by* $x_2' = (x_{2,1}, x_{2,2} \ldots, x_{2,d_2-1})$*. We assume that* $\mathcal{I}' \subseteq \mathbb{C}^{s'}$ *is a minimal semilinear invariant for* A' *and* x'*. Then*

$$\mathcal{I} = \{z \in \mathbb{C}^s \mid z' \in \mathcal{I}' \text{ and } x_{1,d_1} z_{2,d_2} = x_{2,d_2} z_{1,d_1}\} \subseteq \mathbb{C}^s$$

is a minimal semilinear invariant for x, A*.*

Before going on to the proof, let us remark that if $d_2 = 1$, E_{d_2-1,d_1} and $J_{d_2-1}(\lambda)$ are both empty matrices (and the Lemma also holds).

Proof. Clearly $x \in \mathcal{I}$. Let us first check that $\mathcal{I}$ is invariant for A. Let $z \in \mathcal{I}$. Then

$$\begin{aligned}
(Az)' &= \left(A''z'', J_{d_1}(\lambda)z_1, (J_{d_2}(\lambda)z)'\right) \\
&= \left(A''z'', J_{d_1}(\lambda)z_1, (J_{d_2}(\lambda)z)_1, \ldots, (J_{d_2}(\lambda)z)_{d_2-1}\right) \\
&= \left(A''z'', J_{d_1}(\lambda)z_1, (J_{d_2}(\lambda)z)_1, \ldots, (J_{d_2}(\lambda)z)_{d_2-2}, \lambda z_{2,d_2-1} + z_{2,d_2}\right) \\
&= \left(A''z'', J_{d_1}(\lambda)z_1, (J_{d_2}(\lambda)z)_1, \ldots, (J_{d_2}(\lambda)z)_{d_2-2}, \lambda z_{2,d_2-1} + \frac{x_{2,d_2}}{x_{1,d_1}} z_{1,d_1}\right) \\
&= A'z' \in \mathcal{I}',
\end{aligned}$$

and $x_{1,d_1}(Az)_{2,d_2} = x_{1,d_1}\lambda z_{2,d_2} = x_{2,d_2}\lambda z_{1,d_1} = x_{2,d_2}(Az)_{1,d_1}$. Hence $\mathcal{I}$ is invariant for A.

We now show minimality. Let $\mathcal{P}$ be a semilinear invariant containing x. Consider $\mathcal{P}_0 = \mathcal{P} \cap \{z \mid x_{1,d_1}z_{2,d_2} = x_{2,d_2}z_{1,d_1}\}$, and $\mathcal{P}'_0 \subseteq \mathbb{C}^{s'}$ be its projection on all but the last coordinate. We show that $\mathcal{P}'_0$ is invariant for A'. Let $z' \in \mathcal{P}'_0$, and let z be z' extended with $z_{2,d_2} = \frac{x_{2,d_2}}{x_{1,d_1}}z_{1,d_1}$. Then $z \in \mathcal{P}_0$, so $Az \in P_0$. Now, $A'z' = (Az)'$ (the proof for this is similar as that of $\mathcal{I}$'s stability), and so $A'z' \in P'_0$. Hence, $\mathcal{I}' \subseteq P'_0$ by minimality of $\mathcal{I}'$, and so $\mathcal{I} \subseteq \mathcal{P}_0 \subseteq P$.

Through repeated applications of Lemma 33 which reduce the dimension and Lemma 15 which renormalize the reduced instance, we obtain the following theorem.

Theorem 34. *Let A have its eigenvalues $\lambda_1, \ldots, \lambda_s \notin \mathbb{U}$ such that either $\lambda_i = \lambda_j$ or $\lambda_i/\lambda_j \notin \mathbb{U}$, and $x \in \mathbb{C}^s$ which is nonzero on the last coordinate of each block. Then there exists a minimal semilinear invariant for A, x which can be constructed in polynomial time and has polynomial size.*

Proof. If for all $i \neq j$, $\lambda_i \neq \lambda_j$, then they are pairwise non-equivalent, so by Theorem 31, $\mathbb{C}^s$ is the minimal invariant for A and x. Otherwise, we use Lemma 33 on blocks with equal eigenvalues to reduce the dimension, and Lemma 15 to normalize the instance (ensuring that A is in Jordan normal form and x is nonzero on the last coordinate of each block), and easily conclude by induction.

We may now finally extend to the general case.

Theorem 35. *Let A have only eigenvalues of modulus 1 which are not roots of unity, and $x \in \mathbb{C}^s$ with nonzero last coordinates. Then there is an explicit minimal semilinear invariant $\mathcal{I}$ for A and x. In particular, there is a semilinear invariant (namely, $\mathcal{I}$) for $\ell = (A, x, y)$ if and only if $y \notin \mathcal{I}$, which may be decided algorithmically.*

Proof. Let $N \in \mathbb{N}$ be such that A^N is just like in the statement of Theorem 34. Let $\mathcal{I}_0$ be the minimal semilinear invariant for A^N and x. Let

$$\mathcal{I} = \bigcup_{i=0}^{N-1} A^i \mathcal{I}_0.$$

Clearly, $\mathcal{I}$ is semilinear, contains x, and invariant for A. Let $\mathcal{P}$ be a semilinear invariant for A which contains x. Then it is also invariant for A^N, so $\mathcal{I}_0 \subseteq \mathcal{P}$. It follows that $A\mathcal{I}_0, A^2\mathcal{I}_0, \cdots \subseteq \mathcal{P}$, which concludes our proof.

References

1. Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal invariants for linear loops. In *Proceedings of ICALP*, volume 107 of *LIPIcs*, pages 114:1–114:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

2. Alexey Bakhirkin and David Monniaux. Extending constraint-only representation of polyhedra with boolean constraints. In *Proceedings of SAS*, volume 11002 of *Lecture Notes in Computer Science*. Springer, 2018.
3. Jin-Yi Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. Technical report, SUNY at Buffalo, 2000.
4. Jin-Yi Cai, Richard J. Lipton, and Yechezkel Zalcstein. The complexity of the A B C problem. *SIAM J. Comput.*, 29(6):1878–1888, 2000.
5. John W. S. Cassels. *An introduction to Diophantine approximation.* Cambridge University Press, 1965.
6. Robert Clarisó and Jordi Cortadella. The octahedron abstract domain. In *Proceedings of SAS*, volume 3148 of *Lecture Notes in Computer Science*, pages 312–327. Springer, 2004.
7. H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.
8. Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, and Xavier Rival. Why does Astrée scale up? *Formal Methods in System Design*, 35(3):229–264, 2009.
9. Patrick Cousot and Nicolas Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Proceedings of POPL*, pages 84–96. ACM Press, 1978.
10. Jing Dong and Qinghui Liu. Undecidability of infinite post correspondence problem for instances of size 8. *RAIRO - Theoretical Informatics and Applications*, 46(3):451457, 2012.
11. Nathanaël Fijalkow, Pierre Ohlmann, Joël Ouaknine, Amaury Pouly, and James Worrell. Semialgebraic invariant synthesis for the Kannan-Lipton Orbit Problem. In *Proceedings of STACS*, volume 66 of *LIPIcs*, pages 29:1–29:13. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.
12. Nathanaël Fijalkow, Pierre Ohlmann, Joël Ouaknine, Amaury Pouly, and James Worrell. Complete semialgebraic invariant synthesis for the Kannan-Lipton Orbit Problem. *Theory of Computing Systems*, 2019.
13. Khalil Ghorbal, Franjo Ivancic, Gogul Balakrishnan, Naoto Maeda, and Aarti Gupta. Donut domains: Efficient non-convex domains for abstract interpretation. In *Proceedings of VMCAI*, volume 7148 of *Lecture Notes in Computer Science*. Springer, 2012.
14. R. Giacobazzi, F. Logozzo, and F. Ranzato. Analyzing program analyses. In *Proceedings POPL*, pages 261–273. ACM, 2015.
15. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361–416, 2000.
16. Vesa Halava and Tero Harju. Undecidability of infinite Post correspondence problem for instances of size 9. *RAIRO - Theoretical Informatics and Applications - Informatique Théorique et Applications*, 40(4):551–557, 2006.
17. Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. In *Proceedings of LICS*, pages 530–539. ACM, 2018.
18. Ravindran Kannan and Richard J. Lipton. The Orbit Problem is decidable. In *Proceedings of STOC*, pages 252–261, 1980.
19. Ravindran Kannan and Richard J. Lipton. Polynomial-time algorithm for the Orbit Problem. *Journal of the ACM*, 33(4):808–821, 1986.
20. M. Karr. Affine relationships among variables of a program. *Acta Inf.*, 6:133–151, 1976.
21. Z. Kincaid, J. Cyphert, J. Breck, and T. W. Reps. Non-linear reasoning for invariant synthesis. *PACMPL*, 2(POPL):54:1–54:33, 2018.

22. C. Lech. A note on recurring series. *Ark. Mat.*, 2:417–421, 1953.
23. K. Mahler. Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38, 1935.
24. K. Mahler. On the Taylor coefficients of rational functions. *Proc. Cambridge Philos. Soc.*, 52, 1956.
25. Antoine Miné. The octagon abstract domain. In *Proceedings of WCRE*, page 310. IEEE Computer Society, 2001.
26. David Monniaux. On the decidability of the existence of polyhedral invariants in transition systems. *CoRR*, abs/1709.04382, 2017.
27. David Monniaux. On the decidability of the existence of polyhedral invariants in transition systems. *Acta Inf.*, 56(4):385–389, 2019.
28. M. Müller-Olm and H. Seidl. A note on Karr's algorithm. In *Proceedings of ICALP*, volume 3142 of *Lecture Notes in Computer Science*, pages 1016–1028. Springer, 2004.
29. Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *Proceedings of ICALP*, pages 330–341, 2014.
30. Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. Scalable analysis of linear systems using mathematical programming. In *Proceedings of VMCAI*, volume 3385 of *Lecture Notes in Computer Science*, pages 25–41. Springer, 2005.
31. T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen. In *Comptes rendus du congrès des mathématiciens scandinaves*, 1934.