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.*, [20], 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

Monniaux in [25,26] 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.
>
> 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:
>
> 1. $x \in \mathcal{I}_{q_1}$;
> 2. The collection of $\mathcal{I}_q$'s forms an *inductive invariant*: for each transition $q \xrightarrow{t} q'$, we have that $f_t(\mathcal{I}_q \cap g_t) \subseteq \mathcal{I}_{q'}$; and
> 3. $y \notin \mathcal{I}_{q_r}$.
>
> We call such a collection $\{\mathcal{I}_q : q \in Q\}$ a *separating inductive invariant* for program P. (Clearly, the existence of a separating inductive invariant constitutes a proof of non-reachability for P with the given x and y.) 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 $\{\mathcal{I}_q : q \in Q\}$.[6]

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.

---

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

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) could be computed algorithmically [19]. 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 [27], 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 [16].

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 [24], the *octahedron domain* of Clarisó and Cortadella [6], and the *template polyhedra* of Sankaranarayanan *et al.* [29]. In fact, as observed by Monniaux [26], 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 [26]. 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 $x, y \in \mathbb{Q}^d$ 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.

---

[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.

Remark 2. It is worth pointing out that the theorem remains valid even for sufficiently large fixed d (our proof shows undecidability for $d = 336$, but this value could undoubtedly be improved). If moreover one requires $\mathcal{I}$ to be topologically closed, one can lower d to having fixed value 27 (which again is unlikely to be optimal). 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 [26], *"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 [14,13].

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 [10,11] 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 [10,11] in the affirmative:

Theorem 3. *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. *$y \notin \mathcal{I}$.*

Remark 4. The proof shows that, in fixed dimension d, the decision procedure runs in polynomial time. It is worth noting that one also has decidability 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"* [12]. 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* [12]. 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 3, 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 $\mathcal{I}^\circ$, 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

We now define semilinear sets in $\mathbb{C}^d$, by identifying $\mathbb{C}^d$ with $\mathbb{R}^{2d}$. A set $\mathcal{I} \subseteq \mathbb{R}^{2d}$ 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 $\mathbb{C}^d$ of the form

$$\mathcal{H} = \left\{ z \in \mathbb{C}^d \mid \sum_{i=1}^{d} \operatorname{Re}(z\overline{u}) \succ a \right\},$$

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

Lemma 5 (Projections of Semilinear Sets). *Let $\mathcal{I}$ be a semilinear set in $\mathbb{C}^{d+d'}$. Then the projection of $\mathcal{I}$ on the first d coordinates, defined by*

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

is a semilinear set.

Lemma 6 (Sections of Semilinear Sets). *Let $\mathcal{I}$ be a semilinear set in $\mathbb{C}^{d+d'}$ and t in $\mathbb{C}^{d'}$. Then the section of $\mathcal{I}$ along t, defined by*

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

is a semilinear set.

Furthermore, there exists a bound B in $\mathbb{R}$ such that for all t in $\mathbb{C}^{d'}$ of norm at most 1, if $Section(\mathcal{I}, t)$ is non-empty, then it contains some z in $\mathbb{C}^d$ 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 7 (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 overview

We are interested in instances of the Monniaux Problem in which there are no guards, all transitions are affine (or equivalently linear, since affine transitions can be made linear by increasing the dimension of the ambient space by 1), and invariants are semilinear. This gives rise to the *semilinear invariant problem*, where an instance is given by a set of square matrices $A_1, \ldots, A_k \in \mathbb{A}^{d \times d}$ and two points $x, y \in \mathbb{A}^d$. A semilinear set $\mathcal{I} \subseteq \mathbb{C}^d$ is a *separating invariant* if

1. $x \in \mathcal{I}$,
2. $A_i \mathcal{I} \subseteq \mathcal{I}$ for all $i \leq k$,
3. $y \notin \mathcal{I}$.

The semilinear invariant problem asks whether such an invariant exists.

We need to introduce some terminology. The triple $((A_i)_{i \leq k}, x, y)$ is a *reach* instance if there exists a matrix M belonging to the semigroup generated by $(A_i)_{i \leq k}$ such that $Mx = y$, and otherwise it is a *non-reach* instance. Clearly a separating invariant can only exist for non-reach instances. An instance for $k = 1$ is called an *Orbit instance*.

3.1   Undecidability for several matrices

Our first result is the undecidability of the semilinear invariant problem. We start by showing it is undecidable in fixed dimension, with a fixed number of matrices and requiring that the invariant be closed. We defer the proofs until Section 4.

Theorem 8. *The semilinear invariant problem is undecidable for 9 matrices of dimension 3 and closed invariants.*

In establishing the above, we used many matrices of small dimension. One could instead use only two matrices, but increasing the dimension to 27.

Theorem 9. *The semilinear invariant problem is undecidable for 2 matrices of dimension 27 and closed invariants.*

In the above results, it can happen that the target belongs to the closure of the set of reachable points. We now show that we can ignore those "non-robust" systems and maintain undecidability.

Theorem 10. *The semilinear invariant problem is undecidable for "robust" instances,* i.e. *instances in which the target point does not belong to the closure of the set of reachable points.*

The proof of the above result does not require that the invariants be closed. We can therefore establish Theorem 1 by making use of the same construction as in the proof of Theorem 9 to encode all the matrices of Theorem 10 into only two distinct matrices.

3.2   Decidability for simple linear loops

In this section, we are only concerned with Orbit instances. Since it is possible to decide (in polynomial time) whether an Orbit instance is reach or non-reach [17,18], we can always assume that we are given a non-reach instance. All decidability results are only concerned with *closed invariants*, this is crucial in several proofs.

Theorem 11. *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.*

We now comment a few instructive examples to illustrate the different cases that arise. The proof of Theorem 11 is postponed to Section 5.

Example 12. 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 1. 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

$$\mathcal{I} = \{x, Ax\} \cup \operatorname{Conv}\left(\{A^n x, n \leq 8\}\right)^{\mathsf{c}}.$$
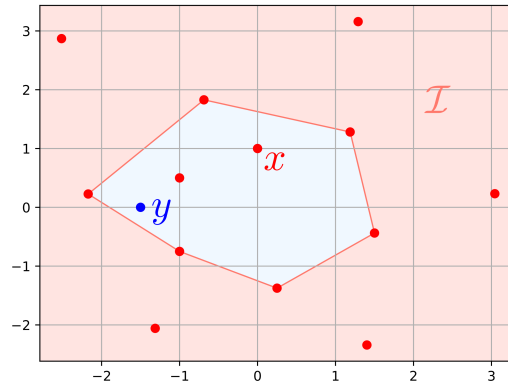
Fig. 1. An invariant for example 12.

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 [10], 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 13. 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 invariants. 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 14. Consider $\ell = (A, x, y)$ in dimension 4 with

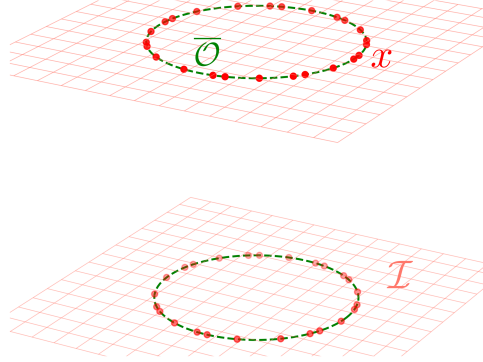$$A = \begin{bmatrix} A' & I_2 \\ 0 & A' \end{bmatrix},$$

where A' is the matrix from Example 13, $x = (0, 0, 1, 0)$ 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 a semialgebraic invariant may easily be constructed.

In examples 13 and 14, 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 12), we will provide a minimal invariant, that is, a semilinear $\mathcal{I}_0$ 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 with two examples having such minimal semilinear invariants.

Example 15. 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 13, 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. Yet the minimal semilinear invariant comprises the union of the two planes containing these circles.

Fig. 2. The minimal invariant for Example 15. Here, $\bar{\mathcal{O}}$ denotes the topological closure of the orbit of x.

Example 16. 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 14. This can be seen as two instances of Example 14 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. Thus, the minimal semilinear invariant in this setting is

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

which has dimension 4. If however, we had $x = (0, 0, 1, 0, 1, 0, -7, 0)$, then the minimal semilinear invariant would be

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

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

4   Undecidability proofs

4.1   Proof of Theorem 8

We reduce an instance of the ω-PCP problem defined as follows: given nine pairs of non-empty words $\{(u^{(1)}, v^{(1)}), \ldots, (u^{(9)}, v^{(9)})\}$ on alphabet $\{0, 2\}$, does

there exist an infinite word $w = w_1 w_2 \ldots$ on alphabet $\{1, \ldots, 9\}$ such that $u^{(w_1)} u^{(w_2)} \cdots = v^{(w_1)} v^{(w_2)} \ldots$. This problem is known to be undecidable [15].

In order to simplify future notations, given a finite or infinite word w, we denote $|w|$ the length of the word w and given an integer $i \leq |w|$, we write w_i for the i'th letter of w. Given a finite or infinite word w on alphabet $\{1, \ldots, 9\}$ we denote $u^{(w)}$ and $v^{(w)}$ the words on the alphabet $\{0, 2\}$ such that $u^{(w)} = u^{(w_1)} u^{(w_2)} \ldots$ and $v^{(w)} = v^{(w_1)} v^{(w_2)} \ldots$. Given a (finite or infinite) word w on the alphabet $\{0, 2\}^*$, denote by $[w] = \sum_{i=1}^{|w|} w_i 4^{1-i}$ the quaternary encoding of w. It is clear that it satisfies $[ww'] = [w] + 4^{-|w|} [w']$ and that $[w] \in [0, \frac{8}{3}]$.

Let $\{(u^{(1)}, v^{(1)}), \ldots, (u^{(9)}, v^{(9)})\}$ be an instance of the ω-PCP problem. For all $i \leq 9$, for readibility, we denote $|u^{(i)}| = n_i$ and $|v^{(i)}| = m_i$. We build the matrices $M_1, \ldots, M_9$ where

$$
M_i = \begin{bmatrix} 1 & [u^{(i)}] & -[v^{(i)}] \\ 0 & 4^{-n_i} & 0 \\ 0 & 0 & 4^{-m_i} \end{bmatrix}
$$

In the following, we write M_w for $w = w_1 \ldots w_k \in \{1, \ldots, 9\}^*$ the matrix $M = M_{w_k} \ldots M_{w_1}$, which can be checked to satisfy

$$
M_w = \begin{bmatrix} 1 & [u^{(w)}] & -[v^{(w)}] \\ 0 & 4^{-|u^{(w)}|} & 0 \\ 0 & 0 & 4^{-|v^{(w)}|} \end{bmatrix}, \qquad M_w \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} [u^w] - [v^w] \\ 4^{-|u^w|} \\ 4^{-|v^w|} \end{bmatrix}.
$$

Let us show that there exists a separating invariant of $((M_i)_{i \leq 9}, x, y)$ where $x = (0, 1, 1)$ and $y = (0, 0, 0)$ iff the ω-PCP instance has no solution.

Let us first assume the ω-PCP instance has a solution w. Fix $r \in \mathbb{N}$ and let $w \!\restriction_r = w_1 \cdots w_r$ and $x_r = M_{w \restriction_r} x$. We have that $x_r = ([u^{(w \restriction_r)}] - [v^{(w \restriction_r)}], 4^{-|u^{(w \restriction_r)}|}, 4^{-|v^{(w \restriction_r)}|})$ and since $u^{(w)} = v^{(w)}$, it is clear that $x_r \to 0 = y$ as $r \to \infty$. Any separating invariant $\mathcal{I}$ must contain this sequence x_r since $\mathcal{I}$ contains the initial point and is stable under $(M_i)_{i \leq 9}$. Moreover, $\mathcal{I}$ is closed so it must contain the limit of the sequence, $(0, 0, 0)$, which is the target point. Thus $\mathcal{I}$ cannot be a separating invariant. Therefore there is no separating invariant of $((M_i)_{i \leq 9}, (0, 1, 1), (0, 0, 0))$.

Now, let us assume the ω-PCP instance has no solution. There exists $n_0 \in \mathbb{N}$ such that for every infinite word w on alphabet $\{0, \ldots, 9\}$ there exists $n \leq n_0$ such that $u_n^{(w)} \neq v_n^{(w)}$. Indeed, consider the tree which root is labelled by $(\varepsilon, \varepsilon)$ and, given a node (u, v) of the tree, if for all $n \leq \min(|u|, |v|)$ we have $u_n = v_n$, then this node has 9 children: the nodes $(uu^{(i)}, vv^{(i)})$ for $i = 1 \ldots 9$. This tree is finitely branching and does not contain any infinite path (which would induce a solution to the ω-PCP instance). Thus, according to König's lemma, it is finite. We can therefore choose the height of this tree as our n_0.

We define the invariant $\mathcal{I} = \mathcal{I}' \cup \mathcal{I}''$ where[8]

$$\mathcal{I}' = \left\{ (s, c, d) : |s| \geq 4(c + d) + 4^{-n_0 - 1} \wedge c \geq 0 \wedge d \geq 0 \right\}$$

and

$$\mathcal{I}'' = \left\{ M_w x : w \in \{1, \ldots, 9\}^* \wedge |w| \leq n_0 + 1 \right\}$$

Let us show that $\mathcal{I}$ is a separating invariant of $((M_i)_{i \leq 9}, (0, 1, 1), (0, 0, 0))$. By definition, $\mathcal{I}$ is closed, semilinear, contains x and does not contain y. The difficult point is to show stability under M_i for $i \leq 9$.

- Let $M_w x \in \mathcal{I}''$, for some w: there are two cases. Either $|w| \leq n_0$, then $|wi| \leq n_0 + 1$, therefore $M_i M_w x = M_{wi} z \in \mathcal{I}''$. Otherwise, $M_i M_w x = M_{wi} x = (s, c, d)$ where $s = \left[u^{(wi)}\right] - \left[v^{(wi)}\right]$, $c = 4^{-|u^{(wi)}|}$ and $d = 4^{-|v^{(wi)}|}$. But then, there exists $n \leq n_0$ such that $u_n^{(wi)} \neq v_n^{(wi)}$. Let n be the smallest such number, then

$$s = \left[u^{(wi)}\right] - \left[v^{(wi)}\right]$$

$$= (u_n^{(wi)} - v_n^{(wi)}) 4^{1-n} + \sum_{j=n+1}^{|wi|} (u_j^{(wi)} - v_j^{(wi)}) 4^{1-j}$$

since $u_j^{(wi)} = v_j^{(wi)}$ for $j < n$. Thus,

$$\begin{aligned} |s| &\geq 2 \cdot 4^{1-n} - \tfrac{8}{3} 4^{-n} && \text{since } |u_n^{(wi)} - u_n^{(wi)}| = 2 \text{ and } [\cdot] \in [0, \tfrac{8}{3}] \\ &\geq 4^{1-n} + 4^{-n} && \\ &\geq 4(c + d) + 4^{-n_0 - 1} && \text{since } n \leq n_0 \text{ and } |u^{(wi)}|, |v^{(wi)}| \geq n_0 + 2. \end{aligned}$$

This shows that $M_i(M_w x) \in \mathcal{I}' \subseteq \mathcal{I}$.

- Let $z = (s, c, d) \in \mathcal{I}'$, then $|s| \geq 4(c+d) + 4^{-n_0-1}$. Without loss of generality, assume that $d \geq c$ (this is completely symmetric in c and d). Let $(s', c', d') = M_i z$, and we check that then

$$\begin{aligned} |s'| &= |s + c\left[u^{(i)}\right] - d\left[v^{(i)}\right]| && \text{by applying the matrix } M_i \\ &\geq |s| - d \max\left(\left[u^{(i)}\right], \left[v^{(i)}\right]\right) && \\ &\geq 4(c+d) + 4^{-n_0-1} - d \max\left(\left[u^{(i)}\right], \left[v^{(i)}\right]\right) && \text{by assumption on } s \\ &\geq 4(c+d) + 4^{-n_0-1} - d\tfrac{8}{3} && \text{since } [\cdot] \in [0, \tfrac{8}{3}] \\ &= 4(c + d/3) + 4^{-n_0-1} && \\ &\geq 4(c' + d') + 4^{-n_0-1} && \text{since } c \geq c' \text{ and } d/4 \geq d' \end{aligned}$$

since $c' = c4^{-|u^{(i)}|}$ and $d' = d4^{-|v^{(i)}|}$. This shows that $M_i z \in \mathcal{I}' \subseteq \mathcal{I}$.

This shows that $\mathcal{I}$ is thus stable and concludes the reduction.

---

[8] This is a semilinear invariant since $|x| \geq y$ if and only if $x \geq y \vee -x \geq y$.

4.2   Proof of Theorem 9

We reduce the instances of Theorem 8 to 2 matrices of size 27. The first matrix M_s shifts upwards the position of the values in the point by 3, while the second matrix M_p applies one of the matrices of the previous reduction, depending on the position of the values within the matrices, then put the obtained value at the top. In other words, $M_p M_s^{i-1}$ for $1 \leq i \leq 9$ intuitively has the same effect as M_i had in the proof of Theorem 8. In the following, we reuse the notations and results of the proof of Theorem 8.

Define matrices M_s and M_p, where I_3 is the identity matrix of size 3×3, and for any $z \in \mathbb{R}^3$ and $i \in \{0, \ldots, 8\}$, the ith shift $z^{\downarrow i} \in \mathbb{R}^{27}$ of z, where $\mathbf{0}_n \in \mathbb{R}^n$ denotes the zero vector of size n, as follows:

$$M_s = \begin{bmatrix} 0 & \cdots & 0 & I_3 \\ I_3 & & & \\ & \ddots & & \\ & & I_3 & 0 \end{bmatrix}, \qquad M_p = \begin{bmatrix} M_1 & \cdots & M_9 \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}, \qquad z^{\downarrow i} = \begin{bmatrix} \mathbf{0}_{3i} \\ z \\ \mathbf{0}_{24-3i} \end{bmatrix}.$$

It follows that $M_s z^{\downarrow i} = z^{\downarrow i+1 \bmod 9}$ and $M_p z^{\downarrow i} = (M_{i+1}z)^{\downarrow 0}$. Assume that there exists a separating invariant $\mathcal{I}$ for $(M_1, \ldots, M_9, x, y)$ and let

$$\mathcal{J} = \bigcup_{i=0}^{8} \{ z^{\downarrow i} : z \in \mathcal{I} \}$$

which is a closed semilinear set. Then for any $z^{\downarrow i} \in \mathcal{J}$, we have $M_s z^{\downarrow i} = z^{\downarrow i+1 \bmod 9} \in \mathcal{I}$ by definition and $M_p z^{\downarrow i} = (M_i z)^{\downarrow 0} \in \mathcal{J}$ since $M_i z \in \mathcal{I}$ by virtue of $z \in \mathcal{I}$ and $\mathcal{I}$ being invariant. Furthermore, $x' = x^{\downarrow 0} \in \mathcal{I}$ since $x \in \mathcal{I}$, and $y' = y^{\downarrow 0} \notin \mathcal{J}$ for otherwise we would have $y \in \mathcal{I}$. Therefore $\mathcal{J}$ is a separating invariant for (M_s, M_p, x', y').

Assume that there exists a separating invariant $\mathcal{J}$ for (M_s, M_p, x', y') and let $\mathcal{I} = \{ z : z^{\downarrow 0} \in \mathcal{J} \}$ which is a closed semilinear set. Clearly $x \in \mathcal{I}$ since $x' = x^{\downarrow 0} \in \mathcal{J}$ and $y \notin \mathcal{I}$ since $y' = y^{\downarrow 0} \notin \mathcal{J}$. Let $z \in \mathcal{I}$ and $i \in \{1, \ldots, 9\}$, then $(M_i z)^{\downarrow 0} = M_p M_s^{i-1} z^{\downarrow 0} \in \mathcal{J}$ and since $z^{\downarrow 0} \in \mathcal{J}$ and $\mathcal{J}$ is invariant under M_s and M_p, thus $M_i z \in \mathcal{I}$. Therefore $\mathcal{I}$ is a non-reachability invariant for $(M_1, \ldots, M_9, x, y)$.

4.3   Proof sketch of Theorem 10

We do the proof of Theorem 10 twice: first we use linear guards in order to limit the selection of the matrices. The added power of the guards allows for a relatively simple proof. This first proof can be seen as an extended sketch of the second one, in Appendix A, where we remove the guards to obtain the result claimed. We do so by emulating the guards using extra variables.

We reduce from the ω-PCP problem and reuse some of the notations of the proof of Theorem 8. Let $\{ (u^{(1)}, v^{(1)}), \ldots, (u^{(9)}, v^{(9)}) \}$ be an instance of the ω-

PCP problem. We build the matrices $\hat{M}_1, \ldots, \hat{M}_9, M_e, M_-$ where

$$
\hat{M}_i = \begin{bmatrix} M_i & \\ & 1\ 2 \\ & 0\ 1 \end{bmatrix}, \qquad M_e = \begin{bmatrix} \mathbf{0}_{3\times3} & \\ & 1\ 0 \\ & 0\ 1 \end{bmatrix}, \qquad M_- = \begin{bmatrix} I_3 & \\ & 1\ -2 \\ & 0\ 1 \end{bmatrix}
$$

and $M_1, \ldots, M_9$ are from the proof of Theorem 8. Moreover, when in (s, c, d, n, a), the matrices $\hat{M}_i$ and M_e can only be selected if the linear guard $|s| < 4(c+d)$ holds, and the matrix M_- can only be selected if $s = c = d = 0$.

Informally, in state (s, c, d, n, a), the subvector (s, c, d) has the same role as before: s contains the difference of the values of the numbers obtained using the v_i and u_i, while c and d are used in order to help compute this value. In the proof of Theorem 8, we showed that when the ω-PCP instance had no solution, there existed a value n_0 such that any pair of words created with the alphabet $(u^{(i)}, v^{(i)})$ differed on one of the first n_0 terms. The variable n is used with the guards in order to detect this value n_0: if such an n_0 exists, then at most $n_0 + 1$ matrices M_i can be selected before the guard stops holding. Moreover, firing a matrix M_i adds 2 to n ensuring that when the guard stops holding, n is smaller or equal to $2(n_0 + 1)$. Conversely, if no such n_0 exist, then there is a way to select matrices M_i such that the guard always holds, allowing the variable n to become an even number as high as one wants. The existence of an upper bound on the value of n is used to build an invariant or to prove that there cannot exist an invariant. Finally, the value a is only here in order to allow for affine modification of the values. It is never modified.

Let $\hat{x} = (x, 0, 1)$ and $\hat{y} = (y, 1, 1)$. Note that $\hat{y}$ is not in the adherence of the reachable set as the fourth variable of any reachable point is an even number while y's is an odd one.

Assume the ω-PCP instance does not possess a solution. Then there exists $n_0 \in \mathbb{N}$ such that any pair of words $(u^{(w)}, v^{(w)})$ differs on one of the first n_0 letters. Define the invariant $\mathcal{I} = \mathcal{I}' \cup \mathcal{I}''$ where

$$
\begin{aligned}
\mathcal{I}' &= \{\hat{M}_w \hat{x} : w \in \{1, \ldots, 9\}^* \wedge |w| \leqslant n_0 + 1\} \\
\mathcal{I}'' &= \{(0, 0, 0, n, 1) : n \leqslant 0 \vee (\exists k \in \mathbb{N}, n = 2k \wedge n \leqslant 2(n_0 + 1))\}.
\end{aligned}
$$

This invariant is clearly semilinear, it contains $\hat{x}$ and does not contain $\hat{y}$. If $z = (0, 0, 0, n, 1) \in \mathcal{I}''$ then only M_- can be triggered due to the guards and $M_- z = (0, 0, 0, n - 2, 1) \in \mathcal{I}''$. Now if $z = (s, c, d, n, a) = \hat{M}_w \hat{x} \in \mathcal{I}'$ for some $w \in \{1, \ldots, 9\}^*$, then M_- cannot be fired as the guard does not hold. If one fires M_e, by construction of $\mathcal{I}'$, n is an even number smaller than $2(n_0 + 1)$, thus $M_e z \in \mathcal{I}''$. Now in order to fire a matrix $\hat{M}_i$, one needs $|s| < 4(c+d)$ to hold. We showed in the proof of Theorem 8 that, from the initial configuration x, after $n_0 + 1$ transitions using one of the matrices M_i then $1/4^{n_0+1} \leqslant |s| - 4(c+d)$. As a consequence, if the guard holds, then $|w| \leqslant n_0$ and $\hat{M}_i z = \hat{M}_{wi} \hat{x} \in \mathcal{I}'$. Therefore, $\mathcal{I}$ is a separating invariant of $(\hat{M}_1, \ldots \hat{M}_9, M_e, M_-, \hat{x}, \hat{y})$.

Now assume the ω-PCP possesses a solution $w \in \{1, \ldots, 9\}^\omega$. For $k \in \mathbb{N}$, we denote $w \restriction_k$ the prefix of length k of w. Let $k \in \mathbb{N}$ and $(s, c, d, n, a) = \hat{M}_{w \restriction_k} x$,

then $|s| < 4(c + d)$. Indeed, assume that $u^{(w \restriction_k)}$ is longer than $v^{(w \restriction_k)}$. Then $u^{(w \restriction_k)} = v^{(w \restriction_k)} t$ for some word $t \in \{0, 2\}^*$ because $u^w (w) v^{(w)}$. Let $\ell = |u^{(w \restriction_k)}|$ and recall that $c = 4^{-\ell}$, then

$$s = |[u^{(w \restriction_k)}] - [v^{(w \restriction_k)}]| = 4^{-\ell}[t] \leqslant 4^{-\ell} \tfrac{8}{3} \leqslant 4c < 4(c + d).$$

The symmetric case is similar but uses d instead. Therefore the guard is satisfied and $M_e \hat{M}_{w \restriction_k} \hat{x} = (0, 0, 0, 2k, 1) \in \mathcal{I}$ is reachable for all $k \in \mathbb{N}$. Let $\mathcal{I}$ be a semi-linear invariant containing the reachability set, then $\mathcal{I} \cap \{(0, 0, 0, x, 1) : x \in \mathbb{R}\}$ is semilinear and contains $(0, 0, 0, 2k, 1)$ for all $k \in \mathbb{N}$. This implies that it nec-essarily contains an unbounded interval and there must exists $k_0 \in \mathbb{N}$ such that $(0, 0, 0, 2k_0 + 1, 1) \in \mathcal{I}$. Since $\mathcal{I}$ is stable by the matrix M_-, $\mathcal{I}$ contains the target y. Therefore, $\mathcal{I}$ is not a separating invariant of $((\hat{M}_1, \dots \hat{M}_9, M_e, M_-), x, y)$.

5 Decidability proofs

This section is aimed at sketching the main ideas of the proof of Theorem 11 while avoiding technicalities and details. We point to the appendix for full proofs. Recall that we only consider closed semilinear invariants.

- We first normalize the Orbit instance, which amounts to putting matrix A in Jordan normal form, and eliminating some easy instances. This is described in Section 5.1.
- We then eliminate some positive cases in Section 5.2. More precisely, we con-struct 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 $y \notin \mathcal{I}$. This part is explained in Section 5.3.

5.1 Normalization

As a first step, recall that every matrix A can be written in the form $A = Q^{-1} J Q$, 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 17. *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. We have:

- $QAQ^{-1}\mathcal{I} \subseteq \mathcal{I}$ 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 17, we can reduce the problem of the existence of semi-linear 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 dimensions of the matrix A are indexed by pairs (J, k), where J ranges over the Jordan blocks and $k \in \{1, \ldots, d(J)\}$ where $d(J)$ is 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 $(J_1, 1)$ (corresponding to the Jordan block J_1) and $(J_2, 1), (J_2, 2)$ (corresponding to the Jordan block J_2).

For a point v and a subset S of $\{1, \ldots, d\}$, let v_S be the projection of v on the dimensions 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 projected on the coordinates of the Jordan block J whose index is greater than k. We write S^c for the coordinates which are not in S.

There are a few degenerate cases which we handle now. We say that an Orbit instance $\ell = (A, x, y)$ in Jordan normal form is normalized if:

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

Lemma 18 is proved in Appendix B.

5.2   Positive cases

Many Orbit instances present a divergence which we can exploit to construct a semilinear invariant. Such behaviours are easily identified once the matrix is in Jordan Normal Form, as properties of its Jordan blocks. We isolate three such cases.

- 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 12). A long enough "initial segment" $\{x, Ax, \ldots, A^k x\}$ together with the complement of its convex hull (on the last coordinate of J) constitutes a semilinear invariant. See Appendix C for details.
- 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, which belongs to the adherence of the orbit on this coordinate. Yet on the full block, $y_J \neq 0$. 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 $||A^k x|| \leq \varepsilon'$. See Appendix D for more details.
- 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 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 build a semilinear invariant. See Appendix E for details.

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

5.3   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 an semilinear invariant, for instance if two synchronised blocks are exactly identical (see Examples 15 and 16 for more elaborate cases).

We start by identifying exactly where semilinear invariants fail. Call two eigenvalues equivalent if their quotient is a root of unity (that is, they have a multiplicative relationship of degree 1). We show that whenever no two different eigenvalues are even non-equivalent, the only stable semilinear sets are trivial. As a consequence, computing the minimal semilinear invariant in this setting is

easy, as it is basically the whole space (except where x is 0). However, this lower bound (non-existence of 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. This is the subject of Appendix F.1.

When the matrix has several equivalent eigenvalues, we show how to iteratively reduce the dimension in order to eventually fall into the previous scenario. Rougly 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, in Appendix F.1.

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. 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.
11. 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.
12. 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.

13. R. Giacobazzi, F. Logozzo, and F. Ranzato. Analyzing program analyses. In *Proceedings POPL*, pages 261–273. ACM, 2015.
14. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361–416, 2000.
15. 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.
16. Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. In *Proceedings of LICS*, pages 530–539. ACM, 2018.
17. Ravindran Kannan and Richard J. Lipton. The Orbit Problem is decidable. In *Proceedings of STOC*, pages 252–261, 1980.
18. Ravindran Kannan and Richard J. Lipton. Polynomial-time algorithm for the Orbit Problem. *Journal of the ACM*, 33(4):808–821, 1986.
19. M. Karr. Affine relationships among variables of a program. *Acta Inf.*, 6:133–151, 1976.
20. Z. Kincaid, J. Cyphert, J. Breck, and T. W. Reps. Non-linear reasoning for invariant synthesis. *PACMPL*, 2(POPL):54:1–54:33, 2018.
21. C. Lech. A note on recurring series. *Ark. Mat.*, 2:417–421, 1953.
22. K. Mahler. Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38, 1935.
23. K. Mahler. On the Taylor coefficients of rational functions. *Proc. Cambridge Philos. Soc.*, 52, 1956.
24. Antoine Miné. The octagon abstract domain. In *Proceedings of WCRE*, page 310. IEEE Computer Society, 2001.
25. David Monniaux. On the decidability of the existence of polyhedral invariants in transition systems. *CoRR*, abs/1709.04382, 2017.
26. David Monniaux. On the decidability of the existence of polyhedral invariants in transition systems. *Acta Inf.*, 56(4):385–389, 2019.
27. 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.
28. Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *Proceedings of ICALP*, pages 330–341, 2014.
29. 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.
30. T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen. In *Comptes rendus du congrès des mathématiciens scandinaves*, 1934.

A   Proof of Theorem 10

We now turn to the second proof without the use of guards. The idea is similar, however, the reduction is far more involved as the use of a guard is now replaced by the test of reachability of additional variables.

We reduce an instance of the ω-PCP problem. Let $\{(u^{(1)}, v^{(1)}), \ldots, (u^{(9)}, v^{(9)})\}$ be an instance of the ω-PCP problem. We denote $|u^{(i)}| = n_i$ and $|v^{(i)}| = m_i$ and we build the matrices $M_1, \ldots M_9, M_m^1, M_m^2, M_x, M_e, M_-, M_p, M_d$ of dimension 21 where:

- for $i = 1\ldots9$, $M_i[1,1] = 1, M_i[1,2] = \left[u^{(i)}\right] = (u_1^{(i)} + u_2^{(i)}/4 + \cdots + u_{n_i}^{(i)}/4^{n_i-1})$, $M_i[1,3] = -\left[v^{(i)}\right]$, $M_i[2,2] = 1/4^{n_i}$, $M_i[3,3] = 1/4^{m_i}$, $M_i[4,4] = 1$, $M_i[4,7] = 2$, $M_i[5,5] = 1$, $M_i[6,6] = 4^{n_i+m_i}$ $M_i[7,7] = 1$ and all other values are set to 0.
- $M_m^1[8,1] = 1$, $M_m^1[8,2] = -4 = M_m^1[8,3]$, $M_m^1[9,1] = 1$, $M_m^1[9,2] = -4 = M_m^1[9,3]$, $M_m^1[9,5] = -1$, $M_m^1[10,1] = 1$, $M_m^1[11,4] = 1$, $M_m^1[12,1] = 1$, $M_m^1[13,6] = 1$, $M_m^1[14,7] = 1$ and all other values are set to 0.
- $M_m^2[8,1] = -1$, $M_m^2[8,2] = -4 = M_m^2[8,3]$, $M_m^2[8,5] = -1$, $M_m^2[9,1] = -1$, $M_m^2[9,2] = -4 = M_m^2[9,3]$, $M_m^2[9,5] = -1$, $M_m^2[10,1] = -1$, $M_m^2[11,4] = 1$, $M_m^2[12,1] = -1$, $M_m^2[13,6] = 1$, $M_m^2[14,7] = 1$ and all other values are set to 0.
- for $i = 8\ldots14$, $M_x[i,i] = 1$, $M_x[8,9] = M_x[10,12] = 1$, $M_x[13,14] = -1$ and all other values are set to 0.
- $M_e[15,8] = M_e[17,10] = M_e[18,11] = M_e[20,13] = M_e[21,14] = 1$ and all other values are set to 0.
- $M_-[18,21] = -2$, for $i = 15\ldots21$, $M_-[i,i] = 1$ and all other values are set to 0.
- $M_p[15,21] = 1$, for $i = 15\ldots21$, $M_p[i,i] = 1$ and all other values are set to 0.
- $M_d[17,21] = -1$, for $i = 15\ldots21$, $M_d[i,i] = 1$ and all other values are set to 0.

Let us explain informally the effects of the different matrices. The dimensions can be separated in three blocs of 7 each. The seven variables associated to the bloc number $i \in \{1,2,3\}$ are called $(s^i, c^i, d^i, n^i, r^i, k^i, a^i)$. As a general overview, the first bloc is used to apply the matrices M_i as in the previous proof (with the guards), the second bloc ensures every value is an integer allowing us, in the third bloc, to use reachability tests in order to verify that the guard of the previous proof holds.

- The matrices M_i only affects the first bloc of variables. On these variables, the effect of these matrices is similar to the effect of the matrices $\tilde{M}_i$ of the extended sketch of proof of the Theorem 10. The one difference comes from the additional variables r^1, which is not used but kept for symmetry with the other blocs, and k^1 which is increased strongly by M_i in a way ensuring that k^1s^1, k^1c^1 and k^1d^1 are integers.
- The matrices M_m^1 and M_m^2 modifies the variables of the bloc 1 and transfer them to the second bloc. Precisely, we have that applying M_m^1 realise the following transformation

$$(s^2, c^2, d^2, n^2, r^2, k^2, a^2) = (s^1 - 4(c^1 + d^1), s^1 - 4(c^1 + d^1), s^1, n^1, s^1, k^1, a^1)$$

and the variables of the bloc 1 are set to 0. M_m^2 has a similar effect, replacing instances of s^1 by $-s^1$.
- The matrix M_x affects the second bloc this way:

$$M_x(s^2, c^2, d^2, n^2, r^2, k^2, a^2) = (s^2 + c^2, c^2, d^2 + r^2, n^2, r^2, k^2 - 1, a^2).$$

Remark that, from the values $(s^2, s^2, d^2, n^2, d^2, k^2, a^2)$ reached after firing one of the matrix M_m^i, using M_x successively k^2 times reaches the values $(k^2 s^2, s^2, k^2 d^2, n^2, d^2, 0, a^2)$. This ensures the first and third variables are now integers.

– M_e moves the variable to the third bloc while putting to 0 two variables that are not useful any more c^3 and r^3 (remark thus than one could simply use matrices of dimension 19 instead of 21. We kept 21 to simplify the representation). In other words, after applying M_e we have

$$(s^3, c^3, d^3, n^3, r^3, k^3, a^3) = (s^2, 0, d^2, n^2, 0, k^2, a^2)$$

and all other variables are set to 0.

– The matrices M_p, M_d and M_- respectively increases by 1, decreases by 1 and decreases by 2 the value of s^3, d^3 and n^3.

The use of these three blocs divides the firing of a sequence of matrices in three steps. The first step corresponds to the firing of the matrices M_i which are the only ones keeping the values within the first dimension bloc. This first step is similar to what was done in the previous proof. Using one of the two matrices M_m^i, $i \in \{1, 2\}$, starts the second step by moving the values to the second bloc (the use of two different matrices is required to represent and check the absolute value in the guard of the previous proof). From now on, the matrices M_i have no effect on the system. The goal of the second, and partially the third, step is to verify whether the guard of the previous proof held when the second step started. To do so, we first use the matrix M_x in order to turn the first two variables into integers. If M_x is not applied an adequate number of times, then the variable labelled by k will never be equal to 0, ensuring non-reachability of the target. We then use the matrix M_e to start the third step. Assuming the multiplication was correctly done, then s^3 and d^3 are now integers. Moreover, $s^3 < 0$ and $d^3 > 0$ iff the guard of the previous proof held when the first step ended. Thus reaching the target on all variables, except for n^3, is possible iff the guard was indeed respected. The case of the counter n^3 is then identical to the one of n in the previous proof.

Let us formally show that there exists a separating invariant of the instance $((M_1, \ldots M_9, M_m^1, M_m^2, M_x, M_e, M_-, M_p, M_d), x, y)$ with $x \in \{(0, 1, 1, 0, 1, 1, 1)\} \times \{0\}^{14}$ and $y \in \{0\}^{14} \times \{(-1, 0, 0, 1, 0, 0, 1)\}$ iff the ω-PCP has no solution.

Assume first that the ω-PCP does not possess a solution. There thus exists $n_0 \in \mathbb{N}$ such that any pair of words $(u^{(w)}, v^{(w)})$ on $\{0, 2\}$ generated from the ω-PCP instance differs on one of the first n_0 letters.

We define the invariant $I = I_1 \cup I_2 \cup I_3$ where

– $I_1 = \{M_w x \mid w \in \{1, \ldots, 9\}^* \wedge |w| \leq n_0 + 1\} \cup \{(s^1, c^1, d^1, n^1, r^1, k^1, 1) \mid |s^1| \geq 4(c^1 + d^1)\} \times \{0\}^{14}$.

– $I_2 = \{M_x^j M_m^i M_w x \mid i \in \{1, 2\} \wedge j \in \mathbb{N} \wedge w \in \{1, \ldots, 9\}^* \wedge |w| \leq n_0 + 1\} \cup \{0\}^7 \times \{(s^2, c^2, d^2, n^2, r^2, k^2, 1) \mid k^2 \leq -1 \vee (d^2 < 0 \wedge r^2 < 0) \vee (s^2 \geq 0 \wedge c^2 \geq 0)\} \times \{0\}^7$.

I_2 is semilinear: while the first set is technically an infinite set of points,

when j is high enough, the variable k^2 becomes negative, ensuring that the point belongs to the second set of I_2 (which is clearly semilinear). Thus the first set only adds to I_2 a finite number of points. It is not closed however. This is not important in this proof as we do not require this condition here. $\overline{I_2}$ could also be used, but would require some additional arguments.

– $I_3 = \{M_p^{j_2} M_d^{j_3} M_-^{j_4} M_e M_x^{j_1} M_m^i M_w x \mid i \in \{1,2\} \wedge j_1, j_2, j_3, j_4 \in \mathbb{N} \wedge w \in \{1, \dots, 9\}^* \wedge |w| \leq n_0 + 1\} \cup \{0\}^{14} \times \{(s^3, c^3, d^3, n^3, r^3, k^3, 1) \mid k^3 \leq 1 \vee n^3 \leq 0 \vee s^3 \geq 0 \vee d^3 < 0\}$.

As for I_2, the first set represents an infinite number of points, but which all reach the second set after a bounded number of steps.

This invariant contains the initial configuration but not the target. It is semilinear. Let us show that it is stable.

Let $h \in I$, we denote the variables within h of the block of seven dimensions number $i \in \{1, 2, 3\}$ by $(s^i, c^i, d^i, n^i, r^i, k^i, a^i)$.

• Case $h \in I_1$. If $|s^1| \geq 4(c^1 + d^1)$, then for $i \leq 9$, $M_i h$ satisfies the same property and for $j \in \{1, 2\}$, $M_m^j h \in \{0\}^7 \times \{(s^2, c^2, d^2, n^2, r^2, k^2, 1) \mid (d^2 < 0 \wedge r^2 < 0) \vee (s^2 \geq 0 \wedge c^2 \geq 0)\} \times \{0\}^7 \subseteq I_2$. The other matrices do not modify s^1, c^1 and d^1 ensuring the property still holds. If there exists $w \in \{1, \dots, 9\}^*, |w| \leq n_0 + 1$ such that $h = M_w x$, then for $j \in \{1, 2\}$, $M_m^j h \in I_2$, if $|w| \leq n_0$, for all $i \leq 9$, $M_i h \in I_1$ and if $|w| = n_0 + 1$, then, as seen in the proof of Theorem 8, $|s^1| \geq 4(c^1 + d^1)$. The other matrices do not modify the variables.

• Case $h \in I_2$. Only two matrices can affect h in meaningful ways: M_x and M_e. As M_e transfer the values to the third block without affecting the positivity (or negativity) of s^2, d^2 and k^2, $M_e h \in I_3$. As M_x removes 1 from k^2 and adds c^2 to s^2 and r^2 to d^2, if h satisfies $k^2 \leq -1 \vee (d^2 < 0 \wedge r^2 < 0) \vee (s^2 \geq 0 \wedge c^2 \geq 0)$, then so does $M_x h$. Finally, if h can be written in the form $M_x^j M_m^i M_w x$, then it is immediately also the case for $M_x h$.

• Case $h \in I_3$. The matrices that affect the variables in meaningful ways are M_p, M_d and M_-. As they are commutative and respectively increases by 1, decreases by 1 and decreases by 2 the value of s^3, d^3 and n^3, we have that all $M_p h$, $M_d h$ and $M_- h$ are in I_3.

Thus I is a separating invariant of the instance.

Conversely, assume the ω-PCP possesses a solution $w \in \{1, \dots, 9\}^\omega$. For $z \in \mathbb{N}$, we denote $w \upharpoonright_z$ the prefix of length z of w and $h_z = M_{w \upharpoonright_z} x$. Then for all $z \in \mathbb{N}$, $|s_z^1| < 4(c_z^1 + d_z^1)$ as showed in the proof of Theorem 8. If $s_z^1 \geq 0$ (resp. $s_z^1 < 0$), triggering the sequence of matrices $M_e (M_x)^{k_z^1} M_m^1$ (resp. $M_e (M_x)^{k_z^1} M_m^2$) on h_z one reaches a point $g_z \in \{0\}^{14} \times \{(s^3, 0, d^3, 2z, 0, 0, 1)\}$ where s^3 is a strictly negative integer and d^3 is a positive integer. Therefore, using the matrices M_p and M_d one can reach the point $y_{2z} \in \{0\}^{14} \times \{(-1, 0, 0, 2z, 0, 0, 1)\}$. As this is true for all $z \in \mathbb{N}$, any semilinear invariant I containing all the points y_{2z} contains a point y_m with $m \in \mathbb{N}$ an odd integer. Therefore as I is stable under M_-, it must contains the target and thus is not a separating invariant of $((M_1, \dots M_9, M_m^1, M_m^2, M_x, M_e, M_-, M_p, M_d), x, y)$.

This concludes the reduction.

B   Proof of Lemma 18

Let $\ell = (A, x, y)$ be a non-reach instance in Jordan normal form.

- 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 $\ell' = (A_{J^c}^n, A_{J^c}^k x_{J^c}, y_{J^c})$. Let $\mathcal{I}'$ be an invariant for ℓ'. For $k' \in \{0, \ldots, n-1\}$, we put

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

$\mathcal{I} = \{x, Ax, \ldots, A^{k-1}x\} \cup \bigcup_{k'=0}^{n-1} \mathcal{I}_{k'}$, 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, $y \notin \{x, Ax, \ldots, A^{k-1}x\}$ 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 $k' \in \{1, \ldots, n-1\}$ (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 $A_{J^c}^n \mathcal{I}' \subseteq \mathcal{I}'$.

  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 $A_{J^c}^k x_{J^c} \in \mathcal{I}'$ and $\mathcal{I}'$ is stable for $A_{J^c}^n$. Now, if $y_{J^c} \in \mathcal{I}'$ 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 $A_{J^c}^n x_{J^c} = y_{J^c}$, 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 $y_{J^c} \notin \{A_{J^c}^n x_{J^c}, n \geq n_0\}$, and claim that ℓ is equivalent to $\ell' = (A_{J^c}, A_{J^c}^{n_0} x_{J^c}, y_{J^c})$. Let $\mathcal{I}'$ be a semilinear invariant for ℓ'. Then $\mathcal{I} = \{x, Ax, \ldots, A^{n_0-1}x\} \cup \{z \mid z_{J^c} \in \mathcal{I}'\}$ 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 22 from section D, 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 $A_{J^c}^n x_{J^c} \in \mathcal{I}'$ and $\mathcal{I}'$ is stable for A_{J^c}. Assume that $y_{J^c} \in \mathcal{I}'$, that is, there exists $\tilde{y} \in P$ such that $y_1 = (y_{J^c}, \tilde{y}) \in \mathcal{I}$. Then $d(y, \mathcal{I}) \leq d(y, y_1) = ||\tilde{y}|| \leq \delta/2$ which is a contradiction, so $y_{J^c} \notin \mathcal{I}'$. Finally, $\{A_{J^c}^{n_0} x_{J^c}, A_{J^c}^{n_0+1} x_{J^c}, \ldots, A_{J^c}^{n-1} x_{J^c}\} \cup \mathcal{I}'$ is an invariant for ℓ' which concludes the proof.

C Some eigenvalue has modulus greater than 1

We start with a simple lemma.

Lemma 19. *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 $\mathbb{C}$ $\left(\text{Conv}\left(\{\lambda^i x \mid i \in \{0, \ldots, n\}\}\right)\right)_{n \in \mathbb{N}}$ 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

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

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

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 $\mathrm{Conv}\left(\{\lambda^i x \mid i \in \{0, \ldots, n_0\}\}\right)$.

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

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

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

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

Theorem 20. *Let $\ell = (A, x, y)$ be a normalized Orbit instance in Jordan normal form. Assume that ℓ is a non-reach instance. 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

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

  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 $\left(\mathrm{Conv}\left(\{\lambda^i x_{J,d(J)} \mid i \in \{1, \ldots, n\}\}\right)\right)_{n \in \mathbb{N}}$ of polyhedra in $\mathbb{C}$. Thanks to Lemma 19, 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 $\mathrm{Conv}\left(\{\lambda^i x_{J,d(J)} \mid i \in \{1, \ldots, n_0\}\}\right)$. Let us denote this convex set by C, and let
  $$\mathcal{I} = \{x, Ax, \ldots, A^{n_0}x\} \cup \overline{\{z \in \mathbb{C}^d \mid z_{J,d(J)} \notin C\}}.$$

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

D   Some eigenvalue has modulus less than 1

We start with a simple lemma.

Lemma 21. *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 $\text{Conv}\left(\left\{\lambda^i x \mid i \in \{0,\ldots,n_0\}\right\}\right)$.

We claim that $B(0,|\lambda|^{n_0} \cdot |x|)$ is included in $\text{Conv}\left(\left\{\lambda^i x \mid i \in \{0,\ldots,n_0\}\right\}\right)$. 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 $\text{Conv}\left(\left\{0, \lambda^p x, \lambda^{p+1}x\right\}\right)$.

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 22. *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

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

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 $|\text{Re}\,((Jz)_d)| + |\text{Im}\,((Jz)_d)| \le |\lambda|(|\text{Re}\,(z_d)| + |\text{Im}\,(z_d)|) \le \varepsilon(1 - |\lambda|)^d$. Now if $i < d$, $(Jz)_i = \lambda z_i + z_{i+1}$, so

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

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 $\mathcal{I} = \text{Conv}\left(\{\lambda^i u \mid i \in \{0, \dots, p\}\}\right)$. 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 $B(0, \alpha) \subseteq \text{Conv}\left(\{\lambda^i u \mid i \in \{0, \dots, p\}\}\right)$ 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 $C_{j_0} \subseteq B(0, \alpha) \subseteq \text{Conv}\left(\{C_0, \dots C_{j_0 - 1}\}\right)$. 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,

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

We now let

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

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 23. *Let $\ell = (x, A, y)$ be a normalized Orbit instance. Assume that ℓ is a non-reach instance. 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 22, 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

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

is a semilinear invariant for ℓ.

E   Some non-diagonalisable eigenvalue is a root of unity

Theorem 24. *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

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

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.

F   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.

– We first assume that 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 F.1
  • It is first shown how to deal with 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 F.2: we first treat the case where all equivalent eigenvalues are equal, and then show how to easily reduce to this setting.

F.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 [30], and more general versions were subsequently obtained by Mahler [22,23] and Lech [21].

Theorem 25 (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 26. *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 containes 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 $\emptyset = \{A^n x, n \in \mathbb{N}\}$ of x. There must be i such that $F_i \cap \emptyset$ 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 25 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 [28, 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 27. *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 eignven-values 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 28. *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 $P_J = \pi_{\{(J,d(J))\}}^{-1}(\{0\}) \subseteq \mathbb{C}^d$. 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 F.1.

We start the induction with an intermediate result.

Lemma 29. *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* $\pi_{last}^{-1}(\{0\}) = \prod_J \mathbb{C}^{d(J) - 1} \times \{0\} = \mathcal{Q}$.

Proof. Let $\mathcal{I}$ be a semilinear invariant for A. Consider $\mathcal{I}' = \pi_{last}(\mathcal{I}) \subseteq \mathbb{C}^s$. 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 27. We reduce to the former case.

Indeed, if $\mathcal{I}' \subseteq \cup P'_J$, we let $\mathcal{I}_J = \pi_{last}^{-1}(P'_J)$, 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, $\pi_{last^c}(\mathcal{I} \cap \mathcal{Q}) = \mathbb{C}^{d-s}$. 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 $\pi_{last^c}(\mathcal{I} \cap \mathcal{Q}) = \mathbb{C}^{d-s}$, or $\pi_{last^c}(\mathcal{I} \cap \mathcal{Q}) \subseteq \cup_J \pi_{\{(J,d(J)-1)\}}^{-1}(\{0\})$. 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 6, we may pick these values such that $z^{(n)}$ is bounded. Up to extracting 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 $\delta = \min\left(1, \min_{\{J'' \mid d(J'') = 2 \text{ and } z_{J'', 1} \neq 0\}} \{|z_{J'', 1}|\}\right) > 0$. 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

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

$$\leq |z^{(n)}_{J''_0, 1}| + k(n)|z^{(n)}_{J''_0, 2}| \leq \delta/4 + \left(\frac{\delta}{2|z^{(n)}_{J''_0, 2}|} + 1\right)|z^{(n)}_{J''_0, 2}| \leq \delta.$$

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,

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

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

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 29 in hands, we now move on to the proof of Theorem 28.

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 29, $\mathcal{Q} \subseteq \mathcal{I}$. 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 29 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 $\pi_{\mathrm{last}}^{-1}(\mathcal{H}')$ 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 $B(A^k z, \varepsilon_k) \cap \pi_{\mathrm{last}}^{-1}(\mathcal{H}')$, 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 $\mathcal{H}^\circ$, 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

$k \in \mathbb{N}$,

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

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 $\text{Diag}\{\lambda_1, \ldots, \lambda_s\} C_k \subseteq C_{k+1}$, the claim follows by a easy induction.
- C_k is not all of $\mathbb{C}^s$. For this, let us consider $\overline{\mathcal{I}^c}$, 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 $\text{Diag}(\mathcal{J}_{d(J)}(\lambda_J^{-1}), J \in \mathcal{J})$. Hence Lemma 29 applies to $\overline{\mathcal{I}^c}$. Since $\mathcal{I} \neq \mathbb{C}^s$, $\mathcal{I}^c$ is nonempty, and since it is an open set, it must be fully dimensional. Hence, either $\overline{\mathcal{I}^c} \subseteq \mathcal{Q}$, 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 $\mathcal{H}^o, \partial \mathcal{H}$ 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 F.1, the fact that C has full dimension, and that C is not $\mathbb{C}^s$, we know that C cannot stabilize $\text{Diag}(\lambda_1, \ldots, \lambda_s)$. In particular, there is $\tilde{u} \in C$ such that $\text{Diag}(\lambda_1, \ldots, \lambda_s)\tilde{u} \notin C$. Let $t_0 = \inf\{t \leq 1, \text{Diag}(\lambda_1^t, \ldots, \lambda_s^t)\tilde{u} \notin C\} \geq 0$, and $u = \text{Diag}(\lambda_1^{t_0}, \ldots, \lambda_s^{t_0})\tilde{u} \in C$, since C is closed. Note that for any small enough $\varepsilon > 0, \text{Diag}(\lambda_1^\varepsilon, \ldots, \lambda_s^\varepsilon)u \notin C$. 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 $v \in B(A^{\varphi(0)}z, 2^{-\varphi(N')}\varepsilon_{\varphi(N')}) \cap \pi_{last}^{-1}(\{u\}) \subseteq B(A^{\varphi(0)}z, \varepsilon_{\varphi(0)}) \cap \pi_{\text{last}}^{-1}(C) \subseteq \mathcal{I}$. 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, $A^{\varphi(N')-\varphi(0)}v \in B(A^{\varphi(N')}z, \varepsilon_{\varphi(N')}) \cap \mathcal{I} = B(A^{\varphi(N')}z, \varepsilon_{\varphi(N')}) \cap \pi_{\text{last}}^{-1}(C)$, but $\pi_{\text{last}}(A^{\varphi(N')-\varphi(0)}v) = \text{Diag}(\lambda_1^{\varphi(N')}, \ldots, \lambda_s^{\varphi(N')})u = \text{Diag}(\lambda_1^{\mu_{N'}}, \ldots, \lambda_s^{\mu_{N'}})$, and since $\mu_{N'} \leq \varepsilon_{N'} \leq \varepsilon_N$, we obtain that $\pi_{\text{last}}(A^{\varphi(N')-\varphi(0)}v) \notin C$, a contradiction.

Note that Theorem 28 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 $p_J = \max\{i \le d(J) \mid x_{J,i} \ne 0\}$. In particular, if the instance is reduced, $x_{J,d(J)} \ne 0$ so the minimal seminlinear invariant is $\mathbb{C}^d$.

F.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 30. *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 $x_{1,d_1} \ne 0$ 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 30 which reduce the dimension and Lemma 18 which renormalize the reduced instance, we obtain the following Theorem.

Theorem 31. *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 forall $i \neq j$, $\lambda_i \neq \lambda_j$, then they are pairwise non-equivalent, so by Theorem 28, $\mathbb{C}^s$ is the minimal invariant for A and x. Otherwise, we use Lemma 30 on blocks with equal eigenvalues to reduce the dimension, and Lemma 18 to normalize the instance (ensuring that A is in Jordan normal form and x is nonzero on the last coordinate of each bloc), and easily conclude by induction.

We may now finally extend to the general case.

Theorem 32. *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 31. 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.