On the Decidability of Linear Bounded Periodic Cyber-Physical Systems

Ruggero Lanotte
Università degli Studi dell'Insubria
Como, Italy
ruggero.lanotte@uninsubria.it

Massimo Merro
Università degli Studi di Verona
Verona, Italy
massimo.merro@univr.it

Fabio Mogavero
Università degli Studi di Napoli
Federico II
Napoli, Italy
fabio.mogavero@unina.it

ABSTRACT

Cyber-Physical Systems (CPSs) are integrations of distributed computing systems with physical processes via a networking with actuators and sensors, where feedback loops among the components allow the physical processes to affect the computations and vice versa. Although CPSs can be found in several complex and sometimes critical real-world domains, their verification and validation often relies on *simulation-test systems* rather then *automatic methodologies* to formally verify safety requirements. In this work, we prove the *decidability* of the *reachability problem* for *discrete-time linear CPSs* whose physical process in isolation has a *periodic behavior*, up to an initial transitory phase.

CCS CONCEPTS

• **Theory of computation → Timed and hybrid models**; **Verification by model checking**; • **Computer systems organization →** *Embedded and cyber-physical systems.*

KEYWORDS

linear cyber-physical systems, reachability problem, formal safety verification

ACM Reference Format:
Ruggero Lanotte, Massimo Merro, and Fabio Mogavero. 2019. On the Decidability of Linear Bounded Periodic Cyber-Physical Systems. In *22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC '19), April 16–18, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3302504.3311797

1 INTRODUCTION

Cyber-Physical Systems (CPSs) are integrations of networking and distributed computing systems with physical processes, where feedback loops allow the latter to affect the computations of the former and vice versa. Basically, CPSs have three main components: the *physical plant*, *i.e.*, the physical process that is managed by the CPS; the *logic*, *i.e.*, controllers, IDSs, and supervisors that govern and control the physical process; the *network* to connect plant and logic. The *physical plant* is usually represented by means of two equations: (i) the *evolution equation*, describing the dynamics of the state variables depending on the control actions implemented through *actuators*, and (ii) the *measurement equation*, providing the measurements of the physical state through *sensors*.

The range of applications of CPSs is rapidly increasing and already covers several domains [10]: advanced automotive systems, environmental monitoring, avionics, critical infrastructure control, *etc.* The common feature of these systems is that they are all safety critical and failures may cause catastrophic consequences. Thus, while *numeric simulations* increase the confidence in the safety of these systems, the complexity of CPSs advocate for *automatic methodologies* to formally verify safety requirements.

One of the central problem in the *safety verification* of complex systems is the *reachability* question: can an unsafe state be reached by an execution of the system starting from a given initial state? The *goal* of this paper is precisely to provide a reachability technique for the safety verification of a significant subclass of linear CPSs.

The reachability problem for hybrid automata [3] (a sort of ancestors of CPSs) has been carefully investigated in the past couple of decades and boundaries of decidability have been extensively explored. In particular, it has been shown to be decidable for significant classes of hybrid automata [1, 2, 7–9, 11, 23, 24, 28].

However, in general, reachability remains undecidable even for simple classes, with relatively simple dynamics, such as *linear hybrid automata* [5], in which the dynamics of the variables are defined by linear differential inequalities, when time is continuous, and linear difference inequalities, in the discrete case. Despite such simple dynamics, indeed, these automata are not suitable to algorithmic analysis even when using only 3 continuous variables comparable only to constants [3].

Nevertheless, decidability has been proven for a number of subclasses of linear hybrid automata equipped with either continuous time [4, 7, 8, 22, 23] or discrete time [1, 2, 9, 27].

Most of these decidability results rely on demonstrating the existence of a finite, computable partition of the state space that is *bisimilar* to the original system.

Contribution. In this work, we focus on discrete-time linear CPSs whose physical plant is expressed by means of two difference equations of the form:

$$\begin{aligned} x_{k+1} &= \mathrm{A}x_k + \mathrm{B}u_k + \mathrm{w} \\ y_k &= \mathrm{C}x_k + e_k \end{aligned}$$

The first equation denotes the *evolution law* and returns the next state vector depending on the current state, the input vector, and an offset vector; while the second equation is the *measurement law* returning the measurement vector y_k depending on the current state

HSCC '19, April 16–18, 2019, Montreal, QC, Canada

ACM ISBN 978-1-4503-6282-5/19/04…$15.00
https://doi.org/10.1145/3302504.3311797

itself and possible errors e_k in the measurements. As in hybrid systems, the physical state vector x_k must respect a *system invariant*; here, we also require that the input vector u_k and the measurement vector y_k respect the invariant: if the invariant is violated the CPS reaches a deadlock state. Unlike hybrid systems, the state x_k of a CPSs cannot be directly analyzed: only its measurement y_k can be observed.

As main result, we prove that the reachability problem of linear CPSs with *rational coefficients* can be solved in ExpSpace, under the hypotheses that:

(i) the system invariant is *bounded*;
(ii) the transformation matrix A is *periodic* with *transient h* and *period k*;
(iii) the mathematical conditions triggering the system evolution, the system invariant, and both the initial and the final sets of states are all *polyhedra* with *rational vertices*.

In case the polyhedra in condition (iii) are *rectangular*, *i.e.*, they can be described by means of linear constraints of the form $x \asymp v$, with $\asymp \in \{<, \leq, >, \geq\}$, x a variable, and $v \in \mathbb{Q}$ a rational number, the reachability problem of the resulting CPSs, called *rectangular*,[1] can be solved in PSpace.

Physical processes of this kind have a *periodic behavior* up to an initial transitory phase, and capture a wide class of *conservative processes*. For simplicity, we will call *bounded periodic* those CPSs that meet the conditions above. Many water-tank plants are bounded periodic CPSs; the paper contains a non-trivial water-tank *running example* to help the reader in understanding the complexity of the physical systems we are able to deal with.

Technically, instead of adopting hybrid automata as basic models, we develop a proper formalization for CPSs which is more informative than hybrid automata as we pay particular attention to the representation of physical devices, such as sensors and actuators, and their mathematical treatment. More specifically, in the physical environment of a CPS we report both the evolution and measurement equations, admitting possible errors in the measurements due to sensor precision. Whereas, the cyber controller can test the physical process, by means of a pool of sensors, and influence its evolution by acting on the actuators.

The first step of our reachability result consists in proving a polynomial-time transformation of our CPSs into an equivalent normal form, where the transformation matrix enjoys a number of useful properties similar to those satisfied by an invertible matrix. Then, we describe a ExpSpace (*resp.*, PSpace) decidability procedure of the *reachability/safety problem* for bounded periodic (*resp.*, rectangular) CPSs, which is based on the notion of reachability polyhedric quotient. Intuitively, we want to determine if there exists an execution starting from an initial configuration that reaches a final one. To do this, we describe how to quotient a bounded periodic CPS in such a way that (i) physical states locally behaving in a similar way are grouped into polyhedra, and (ii) the reachability property is preserved. In the general case, we will show that there are at most doubly-exponentially many polyhedra that can be entirely contained in our bounded system invariants. However, in the case of rectangular CPSs, we are able to prove that the number of possible rectangular polyhedra with the same property is at most exponential in the number of physical state variables. Finally, we show that, in case the boundedness requirement on the system invariant is not satisfied, the same problem turns out to be undecidable, even when assuming rectangular constraints, since such systems can simulate a standard two-counter machine [12, 19].

Outline. Section 2 provides a formalization of CPSs, in terms of syntax, operational semantics, and behavioral equivalence. Section 3 specifies the definition of linear periodic CPSs and some subclasses of them. Then, it presents our running water-tank example and proves the correctness of the transformation into the normal forms mentioned above. Section 4 contains the decidability procedure for the reachability/safety problem of bounded periodic CPSs, and the undecidability result in the presence of unbounded invariants. Section 5 draws conclusions and discusses related work.

2 CYBER-PHYSICAL SYSTEMS

From a high-level view point, beside the communication network, a CPS can be seen as consisting of two main parts: (i) a *physical environment*, defining variables, devices, evolution laws, *etc.*; (ii) a *cyber controller* that interacts with the physical devices (sensors and actuators) and manages the interaction with other cyber components. In this section, we provide a formalization of CPSs that preserves a distinction between these two parts via suitable evolution and transition functions. Then, we describe an associated operational semantics in terms of the *graph of dynamics*.

From now on, we shall make use of the following notation: given a function $e : (\mathcal{X} \cup \mathcal{S} \cup \mathcal{A}) \to \mathbb{R}$, we denote by $e_{\mathcal{X}} \triangleq e{\restriction}\mathcal{X}$, $e_{\mathcal{S}} \triangleq e{\restriction}\mathcal{S}$, and $e_{\mathcal{A}} \triangleq e{\restriction}\mathcal{A}$, respectively, the restrictions of e to the subsets $\mathcal{X}$, $\mathcal{S}$, and $\mathcal{A}$ of its domain.

Definition 1 (Cyber-Physical System). *A* cyber-physical system *(CPS, for short)* w.r.t. *the disjoint finite sets of* state variables $\mathcal{X}$, sensors $\mathcal{S}$, *and* actuators $\mathcal{A}$ *is a tuple* $\mathcal{M} = \langle \mathrm{M}, \mathsf{trn}, \mathsf{evl}, \mathsf{msr}, \mathsf{act}, \mathrm{I}, \mathrm{M}_I, \mathrm{M}_F \rangle$ *whose components are defined as prescribed in the following:*

(1) $\mathrm{M} \triangleq \mathrm{C} \times \mathrm{E}$ *is the Cartesian product of a non-empty finite set of* control states C *and a non-empty set of* physical states $\mathrm{E} \subseteq \mathbb{R}^{(\mathcal{X} \cup \mathcal{S} \cup \mathcal{A})}$*;*
(2) $\mathsf{trn} \colon \mathrm{C} \times \mathbb{R}^{\mathcal{S}} \to 2^{\mathrm{C}}$ *is the* transition function *modeling the digital part of the system dynamics;*
(3) $\mathsf{evl} \colon \mathbb{R}^{\mathcal{X}} \times \mathbb{R}^{\mathcal{A}} \to \mathbb{R}^{\mathcal{X}}$ *is the* evolution function *modeling the analogical part of the system dynamics;*
(4) $\mathsf{msr} \colon \mathbb{R}^{\mathcal{X}} \to 2^{\mathbb{R}^{\mathcal{S}}}$ *is the* measurement function *satisfying the constraint* $e_{\mathcal{S}} \in \mathsf{msr}(e_{\mathcal{X}})$*, for all* $e \in \mathrm{E}$*;*
(5) $\mathsf{act} \colon \mathrm{C} \to \mathbb{R}^{\mathcal{A}}$ *is the* actuator function *satisfying the constraint* $e_{\mathcal{A}} = \mathsf{act}(c)$*, for all* $(c, e) \in \mathrm{M}$*;*
(6) $\mathrm{I} \subseteq \mathrm{M}$ *is the* evolution invariant;[2]
(7) $\mathrm{M}_I, \mathrm{M}_F \subseteq \mathrm{M}$ *are the subsets of* initial *and* final states.

The graph of the dynamics $\mathcal{G}_{\mathcal{M}} \triangleq \langle \mathrm{I}, \to \rangle$ *of a CPS* $\mathcal{M}$ *is such that, for all states* $(c, e), (\widehat{c}, \widehat{e}) \in \mathrm{I}$*, it holds that* $(c, e) \to (\widehat{c}, \widehat{e})$ *iff* $\widehat{c} \in \mathsf{trn}(c, e_{\mathcal{S}})$ *and* $\widehat{e}_{\mathcal{X}} = \mathsf{evl}(e_{\mathcal{X}}, \widehat{e}_{\mathcal{A}})$.[3]

Intuitively, a control state $c \in \mathrm{C}$ is an atomic element, while a physical state $e \in \mathrm{E}$ is encoded as a valuation of variables, sensors,

[1] Not to be confused with *rectangular hybrid automata* [8].

[2] Unlike hybrid systems, our invariant also considers sensors and actuators.

[3] Notice that there are no restrictions to impose on the sensor and actuator components of the state $(\widehat{c}, \widehat{e}) \in \mathrm{I} \subseteq \mathrm{M}$, since this one already satisfies the properties $\widehat{e}_{\mathcal{S}} \in \mathsf{msr}(\widehat{e}_{\mathcal{X}})$ and $\widehat{e}_{\mathcal{A}} = \mathsf{act}(\widehat{c})$.

and actuators with real numbers, which we call, in the following, *variable state* for $e_{\mathcal{X}}$, *sensor state* for $e_{\mathcal{S}}$, and *actuator state* for $e_{\mathcal{A}}$, respectively. The transition function, describing the program of the digital component, assigns to each control state $c \in \mathrm{C}$ and sensor state $e_{\mathcal{S}} \in \mathbb{R}^{\mathcal{S}}$ a set of possible next control states $\mathsf{trn}(c, e_{\mathcal{S}}) \subseteq \mathrm{C}$. The evolution function evl, modeling the physical laws, maps the current variable state $e_{\mathcal{X}} \in \mathbb{R}^{\mathcal{X}}$ and an actuator state $e_{\mathcal{A}} \in \mathbb{R}^{\mathcal{A}}$ to the next variable state $\mathsf{evl}(e_{\mathcal{X}}, e_{\mathcal{A}}) \in \mathbb{R}^{\mathcal{X}}$. The measurement function msr associates every variable state $e_{\mathcal{X}} \in \mathbb{R}^{\mathcal{X}}$ with the set of admissible sensor states $\mathsf{msr}(e_{\mathcal{X}}) \subseteq \mathbb{R}^{\mathcal{S}}$; notice that here, as we assume the presence of a measurement error, the function returns a set of admissible sensor states, rather than a single one. The actuator function act simply links each control state $c \in \mathrm{C}$ to the current value of the actuator state $\mathsf{act}(c)$. Finally, the relation $\rightarrow$ allows to determine how the system evolves globally in a single unit of time, in a way that is compatible with both the transition and evolution functions. Observe that, intuitively, the system gets stuck once it reaches a state $(c, e) \in \mathrm{I}$ having no successors inside the invariant, *i.e.*, such that $(\widehat{c}, \widehat{e}) \notin \mathrm{I}$, for all $(\widehat{c}, \widehat{e}) \in \mathrm{M}$ with $\widehat{c} \in \mathsf{trn}(c, e_{\mathcal{S}})$ and $\widehat{e}_{\mathcal{X}} = \mathsf{evl}(e_{\mathcal{X}}, \widehat{e}_{\mathcal{A}})$.

In the following we will use a straightforward trace-based equivalence between cyber-physical systems.

Definition 2 (System Equivalence). *We say that two CPSs $\mathcal{M}_1$ and $\mathcal{M}_2$ are* equivalent *(*w.r.t. *reachability)* iff *(i) a final state is reachable from an initial state in the graph $\mathcal{G}_{\mathcal{M}_1}$, when the same holds for the graph $\mathcal{G}_{\mathcal{M}_2}$ and,* vice versa*, (ii) a final state is reachable from an initial state in $\mathcal{G}_{\mathcal{M}_2}$, when the same holds for $\mathcal{G}_{\mathcal{M}_1}$.*

3 LINEAR CYBER-PHYSICAL SYSTEMS

In this section, we provide a description of a number of classes of linear CPSs with particular emphasis on *bounded periodic* CPSs, whose physical evolution in isolation, after a transitory phase, has a periodic behavior.

Before proceeding, let us fix some notation. By $\cdot$ we denote both the classic matrix/vector product and the operation of product between a matrix A and a set of vectors P of suitable dimensions defined as usual as $\mathrm{A} \cdot \mathrm{P} \triangleq \{\mathrm{A} \cdot e : e \in \mathrm{P}\}$. In addition, the sum of a vector w and a set of vectors P of the same dimensions, also known as translation of P *w.r.t.* the direction w, is defined as $\mathrm{w} + \mathrm{P} = \mathrm{P} + \mathrm{w} \triangleq \{\mathrm{w} + e : e \in \mathrm{P}\}$. We can generalize this to the sum of two sets of vectors as follows: $\mathrm{P}_1 + \mathrm{P}_1 \triangleq \{e_1 + e_2 : \forall i \in \{1, 2\} \,.\, e_i \in \mathrm{P}_i\}$. A square matrix A is *singular* if its determinant is zero, is *nilpotent* if there exists a positive number $\ell \in \mathbb{N}_+$, called *order* of A, such that $\mathrm{A}^{\ell} = \mathbf{0}$, with $\mathbf{0}$ the null matrix, and is *periodic* with *transient* h and *period* k (h, k-periodic, for short) if $\mathrm{A}^{k+h+1} = \mathrm{A}^{h+1}$, with $h, k \in \mathbb{N}$. Finally, it is *h, k-zero padded* if it can be decomposed in blocks as follows, where $\Delta \in \mathbb{R}^{(n-k)\times k}$ is a rectangular matrix, $\Gamma \in \mathbb{R}^{(n-k)\times(n-k)}$ is a square matrix with rank $h \leq n - k$, and $\Lambda \in \mathbb{R}^{k\times k}$ a nilpotent matrix, with $n \in \mathbb{N}_+$ the dimension of A:

$$\mathrm{A} = \left(\begin{array}{c|c} \Gamma & \Delta \\ \hline \mathbf{0} & \Lambda \end{array}\right).$$

The index $\ell \in \mathbb{N}_+$ of a h, k-zero padded matrix is the index of its nilpotent submatrix, which can never exceed its dimension.

We can now introduce the definition of linear CPS, which enforces linearity constraints on the dynamics of the physical component of the system.

Definition 3 (Linear Cyber-Physical System). *A cyber-physical system $\mathcal{M} = \langle \mathrm{M}, \mathsf{trn}, \mathsf{evl}, \mathsf{msr}, \mathsf{act}, \mathrm{I}, \mathrm{M}_I, \mathrm{M}_F \rangle$* w.r.t. *the disjoint finite sets of* state variables $\mathcal{X}$*,* sensors $\mathcal{S}$*, and* actuators $\mathcal{A}$ *is* linear *if it satisfies the following four properties, where $n_{\mathcal{X}} \triangleq |\mathcal{X}|$, $n_{\mathcal{S}} \triangleq |\mathcal{S}|$, and $n_{\mathcal{A}} \triangleq |\mathcal{A}|$:* [4]

1. *there exists a partition of $\mathbb{R}^{n_{\mathcal{S}}} = \mathrm{P}_1 \uplus \cdots \uplus \mathrm{P}_m$ into $m \in \mathbb{N}$ polyhedra $\mathrm{P}_1, \ldots, \mathrm{P}_m \subseteq \mathbb{R}^{n_{\mathcal{S}}}$, called* condition polyhedra*, such that $\mathsf{trn}(c, e_{\mathcal{S}1}) = \mathsf{trn}(c, e_{\mathcal{S}2})$, for all $c \in \mathrm{C}$, $i \in [1, m]$, and $e_{\mathcal{S}1}, e_{\mathcal{S}2} \in \mathrm{P}_i$;*
2. *there exist a square matrix $\mathrm{A} \in \mathbb{R}^{n_{\mathcal{X}}\times n_{\mathcal{X}}}$, a rectangular matrix $\mathrm{B} \in \mathbb{R}^{n_{\mathcal{X}}\times n_{\mathcal{A}}}$, and a vector $\mathrm{w} \in \mathbb{R}^{n_{\mathcal{X}}}$, called* transformation matrix*,* actuator matrix*, and* offset vector,[5] *respectively, such that $\mathsf{evl}(e_{\mathcal{X}}, e_{\mathcal{A}}) = \mathrm{A} \cdot e_{\mathcal{X}} + \mathrm{B} \cdot e_{\mathcal{A}} + \mathrm{w}$;*
3. *there exist a rectangular matrix $\mathrm{C} \in \mathbb{R}^{n_{\mathcal{S}}\times n_{\mathcal{X}}}$ and a polyhedron $\mathrm{D} \subseteq \mathbb{R}^{n_{\mathcal{S}}}$, called* sensor matrix *and* error polyhedron*, respectively, such that $\mathsf{msr}(e_{\mathcal{X}}) = \mathrm{C} \cdot e_{\mathcal{X}} + \mathrm{D}$;*
4. *the evolution invariant* I *can be decomposed as the Cartesian products $\mathrm{C}^* \times \mathrm{F}^* \times \mathrm{G}^*$ of a set of control states $\mathrm{C}^* \subseteq \mathrm{C}$, a polyhedron $\mathrm{F}^* \subseteq \mathbb{R}^{n_{\mathcal{X}}+n_{\mathcal{S}}}$ on the variable and sensor states, and a finite set of actuator states $\mathrm{G}^* \subset \mathbb{R}^{n_{\mathcal{A}}}$.*
5. *the sets of initial and finite states M_α with $\alpha \in \{I, F\}$ can be decomposed as the Cartesian products $\mathrm{C}_\alpha \times \mathrm{F}_\alpha \times \mathrm{G}_\alpha$ of sets of control states $\mathrm{C}_\alpha \subseteq \mathrm{C}$, polyhedra $\mathrm{F}_\alpha \subseteq \mathbb{R}^{n_{\mathcal{X}}+n_{\mathcal{S}}}$, and finite sets of actuator states $\mathrm{G}_\alpha \subset \mathbb{R}^{n_{\mathcal{A}}}$.*

$\mathcal{M}$ is rational *if the matrices* A*,* B*, and* C*, the vector* w*, and the vertices of the polyhedra* D*, F^*, F_I, and F_F are all rational. Moreover, $\mathcal{M}$ is* bounded *(*resp.*,* singular*,* nilpotent*, h, k-*zero padded*, or h, k-*periodic*, with $h, k \in \mathbb{N}$) if F^* is bounded* [6] *(*resp.*,* A *is singular, nilpotent, h, k-zero padded, or is periodic with transient h and period k).*

Intuitively, a CPS is linear if both the evolution and the measurement functions, as well as the sets of initial and final states and the invariant, can be described by means of linear equations/inequalities. It is also rational if the coefficients used in these equations/inequalities are rational and it is bounded if all the values associated with the variables, sensors, and actuators are *a priori* bounded during the entire evolution of the physical system. Finally, it is periodic, if, after a transient, the free evolution of the environment is periodic, *i.e.*, the state variable values change in a periodic way under the action of the transformation matrix, and it is singular, nilpotent, or h, k-zero padded if this matrix enjoys precisely the same properties.

As an example of physical system, consider a water-tank plant as depicted in Figure 1, where the volume of each tank is 100 liters. In any unit of time, due to an always-on pump, the water in Tank T1 flows completely into Tanks T2 and T3 with a ratio of 3 to 1 in favor of the first. Because of some losses along the pipe before the bifurcation, 1 liter of this water gets lost. Still in one time

[4] From now on, with an abuse of notation, given an arbitrary finite set $\mathcal{N}$ of $n_{\mathcal{N}}$ elements, we identify the two isomorphic sets $\mathbb{R}^{\mathcal{N}}$ and $\mathbb{R}^{n_{\mathcal{N}}}$.

[5] For simplicity, we assume a perturbation of the physical evolution represented in terms of a simple offset that affects the evolution in a constant manner.

[6] Observe that the invariant I is bounded *iff* the associated polyhedron F^* is bounded as well, due to the fact that the set of actuator states G^* is finite.

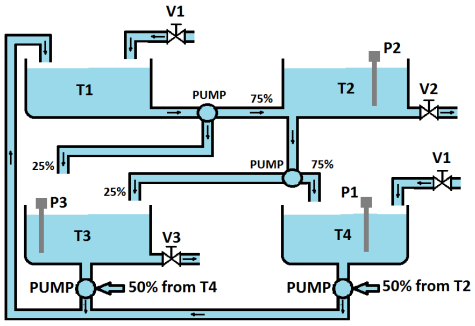

Figure 1: Water Tank Plant $\mathcal{M}_{WT}$.

unit, the content of Tank T2 is completely pumped into Tanks T3 and T4, again with a ratio of 3 to 1 in favor of the second. Of the water directed to Tank T4, 0.5 liters gets lost. At the same time, due to an elevation gain of Tanks T3 and T4 *w.r.t.* Tank T1, the water of the first two tanks completely flows into the third one; this automatically actuates two pumps that transfer half of the contents of Tanks T4 and T2 into Tank T1. Through the three-position Valve V1, a controller can introduce from an external water supply network 5, 2.5, or 0 liters of water, per time unit, in both Tanks T1 and T4, simultaneously. Via the on/off Valves V2 and V3, a controller can remove 7.5 and 3 liters from Tanks T2 and T3, respectively. The quantity of water in the Tanks T2, T3 and T4 can be measured through three electric linearly-proportional probes with a 1% precision *w.r.t.* the maximum scale value. Probe P1 transforms the water level of Tank T4, actually its volume, into an electric signal in the range from 0 to 12 volts, while Probes P2 and P3 do the same in the range from 0 to 5 volts for the Tanks T2 and T3, respectively. Finally, in the initial state of the plant each tank contains about 25 liters of water with a precision of 5%, and all valves are shut off. Moreover, as critical states, *i.e.*, states outside the invariant, we consider those where all tanks are empty and, at the same time, Valve V1 for external supply is shut off.

As an example of digital controller for the physical system described above, we can consider a simple one that nondeterministically chooses among the following two actions:

- if Probe P1 returns a signal whose value is lower than 6 volts but greater than 3 volts, the controller opens half of the Valve V1; if the value is lower than or equal to 3, then it opens the valve completely; in all other cases such a valve is shut off;
- if Probe P2 (*resp.*, Probe P3) returns a value greater than 2.5 volts, the controller opens Valve V2 (*resp.*, Valve-V3), otherwise, it is shut off.

This tank plant in its entirety can be modeled by means of a rational CPS $\mathcal{M}_{WT} = \langle \mathrm{M}, \mathrm{trn}, \mathrm{evl}, \mathrm{msr}, \mathrm{act}, \mathrm{I}, \mathrm{M}_I, \mathrm{M}_F \rangle$ as follows, where the quantity of water in the tanks is represented via the variables x_1, x_2, x_3, and x_4, the probes via the sensors s_1, s_2, and s_3, and the valves via the corresponding actuators a_1, a_2, and a_3:

- the finite set of control states can be represented as $\mathrm{C} = \{c_0\} \cup 2^{\{\mathrm{P1} \leq 3,\ 3 < \mathrm{P1} < 6,\ \mathrm{P2} > 2.5,\ \mathrm{P3} > 2.5\}}$, where c_0 is the initial control state, while the other ones denote all the possible distinguishable evaluations of the three probes;
- the physical states in E are isomorphically represented as points in the $\mathbb{R}^{10}$ vector space, where the first four coordinates identifies the variables x_1, x_2, x_3, and x_4, the second three the sensors s_1, s_2, and s_3, and the last ones the actuators a_1, a_2, and a_3;
- $\mathrm{trn}(c, e_{\mathcal{S}}) \triangleq \{c_0\}$, if $e_{\mathcal{S}}(s_1) \geq 6$, $e_{\mathcal{S}}(s_2) \leq 2.5$, and $e_{\mathcal{S}}(s_3) \leq 2.5$, while $\mathrm{trn}(c, e_{\mathcal{S}})$ contains the proposition $\mathrm{Pi} \asymp v$ *iff* the value $e_{\mathcal{S}}(s_i)$ read on the sensor s_i satisfies the relation $\asymp v$, *e.g.*, $\mathrm{P1} \leq 3 \in \mathrm{trn}(c, e_{\mathcal{S}})$ *iff* $e_{\mathcal{S}}(s_1) \leq 3$;
- the transformation and actuator matrices together with the offset vector are

$$\mathrm{A} = \begin{pmatrix} 0 & 0 & 1.5 & 1.5 \\ 0.75 & 0 & 0 & -0.5 \\ 0.25 & 0.25 & 0 & 0 \\ 0 & 0.75 & -0.5 & 0 \end{pmatrix}, \mathrm{B} = \begin{pmatrix} 5 & 0 & 0 \\ 0 & -7.5 & 0 \\ 0 & 0 & -3 \\ 5 & 0 & 0 \end{pmatrix}, \mathrm{w} = \begin{pmatrix} 0 \\ -0.75 \\ -0.25 \\ -0.50 \end{pmatrix};$$

- the error polyhedron D is $[-0.12, 0.12] \times [-0.05, 0.05] \times [-0.05, 0.05]$, while the sensor matrix is

$$\mathrm{C} = \begin{pmatrix} 0 & 0 & 0 & 0.12 \\ 0 & 0.05 & 0 & 0 \\ 0 & 0 & 0.05 & 0 \end{pmatrix},$$

- $\mathrm{act}(c_0)(a) \triangleq 0$, for all $a \in \{\mathrm{V1}, \mathrm{V2}, \mathrm{V3}\}$; $\mathrm{act}(c)(\mathrm{V1}) \triangleq 1$ *iff* $\mathrm{P1} \leq 3 \in c$; $\mathrm{act}(c)(\mathrm{V1}) \triangleq 0.5$ *iff* $3 < \mathrm{P1} < 6 \in c$; $\mathrm{act}(c)(\mathrm{V2}) \triangleq 1$ *iff* $\mathrm{P2} > 2.5 \in c$; $\mathrm{act}(c)(\mathrm{V3}) \triangleq 1$ *iff* $\mathrm{P3} > 2.5 \in c$.
- the invariant I is the Cartesian product of the control state set C with the following intervals of values: $[0, 100]$ for the state variables, $[-0.12, 12.12]$ for the first sensor, $[-0.05, 5.05]$ for the other two sensors, $\{0, 0.5, 1\}$ for the first actuator, and $\{0, 1\}$ for the other two actuators;
- the set of initial states M_I is the Cartesian product of the singleton $\{c_0\}$ with the following intervals of values: $[23.75, 26.25]$ for the variables, $[2.73, 3.27]$ for the first sensor, $[1.1375, 1.3625]$ for the other two sensors, and $\{0\}$ for the actuators;
- the set of finals states M_F is the Cartesian product of the control state set C with the following intervals of values: $\{0\}$ for the variables, $[-0.12, 0.12]$ for the first sensor, $[-0.05, 0.05]$ for the other two sensors, $\{0\}$ for the first actuator, and $\{0, 1\}$ for the other two actuators.

It is interesting to notice that the just described CPS $\mathcal{M}_{WT}$ is also bounded, singular, 3, 0-zero padded, and 0, 3-periodic. Thus, the system under consideration does not have a transitory phase. Had we added n extra tanks in cascade, with the last one which uniformly distributes its content to Tanks T1, T2, T3, and T4, we would have had a n, 3-periodic system.

In the following, we make use of the well-known notion of matrix similarity: two square matrices $\mathrm{A}_1, \mathrm{A}_2 \in \mathbb{R}^{n \times n}$ are *similar* if there exists an invertible matrix $\mathrm{P} \in \mathbb{R}^{n \times n}$ such that $\mathrm{A}_2 = \mathrm{P}^{-1} \cdot \mathrm{A}_1 \cdot \mathrm{P}$.

Once all necessary mathematical machinery about linear CPS has been defined, we are ready prove the first technical result about how to modify the transformation matrix A in order to get an invertible sub-matrix Γ. This will be necessary to put the original linear CPS in a proper normal form suitable for the decision procedure described later in this article.

Lemma 1 (Zero-Padded Matrices). *For every i, j-zero-padded (rational, h, k-periodic) square matrix $\mathrm{A} \in \mathbb{R}^{n \times n}$, with $i + j < n$, there*

exists a similar i^*, $(j+1)$-zero-padded (rational, h,k-periodic) square matrix $\widetilde{\mathsf{A}} \in \mathbb{R}^{n\times n}$, for some $i^* \leq n-j-1$.

Proof. Since $i+j<n$, the matrix $\mathsf{A}\in\mathbb{R}^{n\times n}$ can be rewritten, *w.l.o.g.*, as a block matrix of the form

$$\mathsf{A}=\left(\begin{array}{c|c}\Gamma & \Delta\\ \hline \mathbf{0} & \Lambda\end{array}\right),\ \Gamma=\left(\begin{array}{c|c}\Xi & \Xi\cdot\mu_c\\ \hline \mu_r^{\mathsf{T}}\cdot\Xi & \mu_r^{\mathsf{T}}\cdot\Xi\cdot\mu_c\end{array}\right),\ \Delta=\left(\begin{array}{c}\Psi\\ \hline \psi^{\mathsf{T}}\end{array}\right),$$

where $\Xi\in\mathbb{R}^{(n-j-1)\times(n-j-1)}$, $\Psi\in\mathbb{R}^{(n-j-1)\times j}$, and $\Lambda\in\mathbb{R}^{j\times j}$ are three matrices, the last one of which is nilpotent, $\mu_r,\mu_c\in\mathbb{R}^{n-j-1}$ and $\psi\in\mathbb{R}^{j}$ are three vectors, and T is the transposition operation. Intuitively, we are expressing the first $n-j$ components of the $(n-j)$-th row and column of A as a linear combination of the same components of its first $n-j-1$ rows and columns, respectively, where the corresponding coefficients are grouped into the vectors μ_r and μ_c. This is possible as the square submatrix Γ composed of the first $n-j$ rows and columns of A has rank i smaller than its dimension.

Now, consider the following modified matrix $\widetilde{\mathsf{A}}\in\mathbb{R}^{n\times n}$, where I is the identity matrix of dimension $n-j-1$ and $\otimes$ the operation of outer product between a column vector and a row one:

$$\widetilde{\mathsf{A}}\triangleq\left(\begin{array}{c|c}\widetilde{\Gamma} & \widetilde{\Delta}\\ \hline \mathbf{0} & \widetilde{\Lambda}\end{array}\right),\ \widetilde{\Gamma}\triangleq\Xi\cdot(\mathsf{I}+\mu_c\otimes\mu_r^{\mathsf{T}}),\ \widetilde{\Delta}\triangleq\left(\Xi\cdot\mu_c\ \middle|\ \Psi\right),$$

$$\widetilde{\Lambda}\triangleq\left(\begin{array}{c|c}0 & \psi^{\mathsf{T}}-\mu_r^{\mathsf{T}}\cdot\Psi\\ \hline \mathbf{0} & \Lambda\end{array}\right).$$

It is not hard to see that $\widetilde{\mathsf{A}}$ is $i^*,(j+1)$-zero padded, for some $i^*\leq n_{\mathcal{X}}-j-1$. Indeed, $i^*=\mathrm{rank}(\widetilde{\Gamma})\leq n_{\mathcal{X}}-j-1$, since $\widetilde{\Gamma}$ has dimension $n_{\mathcal{X}}-j-1$. In addition, the $(j+1)$-dimensional square submatrix $\widetilde{\Lambda}$ of $\widetilde{\mathsf{A}}$ composed of its last $j+1$ rows and columns is nilpotent, since Λ is nilpotent as well:

$$\left(\begin{array}{c|c}0 & \lambda^{\mathsf{T}}\\ \hline \mathbf{0} & \Lambda\end{array}\right)^{\ell+1}=\left(\begin{array}{c|c}0 & \lambda^{\mathsf{T}}\cdot\Lambda^{\ell}\\ \hline \mathbf{0} & \Lambda\cdot\Lambda^{\ell}\end{array}\right)=\left(\begin{array}{c|c}0 & \lambda^{\mathsf{T}}\cdot\mathbf{0}\\ \hline \mathbf{0} & \Lambda\cdot\mathbf{0}\end{array}\right)=\mathbf{0},$$

where ℓ is the degree of Λ, and $\lambda^{\mathsf{T}}=\psi^{\mathsf{T}}-\mu_r^{\mathsf{T}}\cdot\Psi$.

At this point, to conclude the proof, one can observe by direct computation that A and $\widetilde{\mathsf{A}}$ are similar, *i.e.*, $\widetilde{\mathsf{A}}=\mathsf{P}^{-1}\cdot\mathsf{A}\cdot\mathsf{P}$, via the following invertible matrix $\mathsf{P}\in\mathbb{R}^{n\times n}$:

$$\mathsf{P}\triangleq\left(\begin{array}{c|c|c}\mathsf{I} & \mathbf{0} & \mathbf{0}\\ \hline \mu_r^{\mathsf{T}} & 1 & \mathbf{0}\\ \hline \mathbf{0} & \mathbf{0} & \mathsf{I}\end{array}\right),\ \text{with}\ \mathsf{P}^{-1}=\left(\begin{array}{c|c|c}\mathsf{I} & \mathbf{0} & \mathbf{0}\\ \hline -\mu_r^{\mathsf{T}} & 1 & \mathbf{0}\\ \hline \mathbf{0} & \mathbf{0} & \mathsf{I}\end{array}\right),$$

where the two identity matrices along the principal diagonal have dimension $n_{\mathcal{X}}-j-1$ and j, respectively.

Finally, notice that $\widetilde{\mathsf{A}}$ is obviously rational, if A is rational. Moreover, the periodicity of the latter is preserved in the former. Indeed, suppose that A is h,k-periodic, *i.e.*, $\mathsf{A}^{k+h+1}=\mathsf{A}^{h+1}$. Then, $\widetilde{\mathsf{A}}^{k+h+1}=(\mathsf{P}^{-1}\cdot\mathsf{A}\cdot\mathsf{P})^{k+h+1}=\mathsf{P}^{-1}\cdot\mathsf{A}^{k+h+1}\cdot\mathsf{P}=\mathsf{P}^{-1}\cdot\mathsf{A}^{h+1}\cdot\mathsf{P}=(\mathsf{P}^{-1}\cdot\mathsf{A}\cdot\mathsf{P})^{h+1}=\widetilde{\mathsf{A}}^{h+1}$, since $\mathsf{P}^{-1}\cdot\mathsf{A}^{n}\cdot\mathsf{P}=(\mathsf{P}^{-1}\cdot\mathsf{A}\cdot\mathsf{P})^{n}$, for any $n\in\mathbb{N}$. Thus, $\widetilde{\mathsf{A}}$ is h,k-periodic as well. □

Before proceeding, we observe that the Jordan canonical form [20] provides an effective way to characterize periodic matrices. Formally, a square matrix A is h,k-periodic *iff*

- it is diagonalizable on the complex field $\mathbb{C}$,
- all non-null eigenvalues are $(k-1)$-th roots of the unit, and
- 0 is one of its eigenvalues with multiplicity h, when $h>0$.

Therefore, to determine the period k and the transient h of A it is enough to analyze its characteristic polynomial and verify whether it can be decomposed in the form $\lambda^h(\lambda-\lambda_0)^{m_0}\cdots(\lambda-\lambda_n)^{m_n}$, for some numbers $n,m_0,\ldots,m_n\in\mathbb{N}$, where all λ_i are complex $(k-1)$-th roots of 1. Then, by exploiting the knowledge on the eigenvalues $0,\lambda_0,\ldots,\lambda_n$, one can check if A is diagonalizable by using the standard null-space algorithm. Notice that part of this process is automatically done by the normalization procedure behind the proofs of Lemma 1, which automatically returns the transient h, so, one can just focus on the non-singular submatrix Γ of A.

Thanks to the above lemma, we can now derive the following theorem allowing us to show that, for every CPS $\mathcal{M}$ having a transformation matrix A with a singular non-nilpotent part Γ, there exists an equivalent CPS $\widetilde{\mathcal{M}}$ whose transformation matrix $\widetilde{\mathsf{A}}$ has a non-singular non-nilpotent part $\widetilde{\Gamma}$.

Theorem 1 (Zero-Padded CPSs). *For every i,j-zero-padded (rational, bounded, h,k-periodic) CPS $\mathcal{M}$ on $n_{\mathcal{X}}$ variables, with $i+j<n_{\mathcal{X}}$, there exists an equivalent i^*, $(j+1)$-zero-padded (rational, bounded, h,k-periodic) CPS $\widetilde{\mathcal{M}}$, for some $i^*\leq n_{\mathcal{X}}-j-1$.*

Proof. Let $\mathcal{M}=\langle \mathrm{M},\mathsf{trn},\mathsf{evl},\mathsf{msr},\mathsf{act},\mathrm{I},\mathrm{M}_I,\mathrm{M}_F\rangle$ and consider the $i^*,(j+1)$-zero padded CPS $\widetilde{\mathcal{M}}=\langle\widetilde{\mathrm{M}},\mathsf{trn},\widetilde{\mathsf{evl}},\widetilde{\mathsf{msr}},\mathsf{act},\widetilde{\mathrm{I}},\widetilde{\mathrm{M}_I},\widetilde{\mathrm{M}_F}\rangle$ with the same cyber controller as $\mathcal{M}$, but a new physical environment defined as follows, where the transformation matrix $\widetilde{\mathsf{A}}$ is computed, via Lemma 1, as $\widetilde{\mathsf{A}}\triangleq\mathsf{P}^{-1}\cdot\mathsf{A}\cdot\mathsf{P}$, for some invertible matrix $\mathsf{P}\in\mathbb{R}^{n_{\mathcal{X}}\times n_{\mathcal{X}}}$:

- the set of states $\widetilde{\mathrm{M}}\triangleq\mathrm{C}\times\widetilde{\mathrm{E}}$ is the product of the original set of control states C with the set of the physical states $\widetilde{\mathrm{E}}$ containing exactly those vectors $\widetilde{e}\in\mathbb{R}^{n_{\mathcal{X}}+n_{\mathcal{S}}+n_{\mathcal{A}}}$ for which there exists a physical states $e\in\mathrm{E}$ such that: (i) $\widetilde{e}_{\mathcal{X}}=\mathsf{P}^{-1}\cdot e_{\mathcal{X}}$, (ii) $\widetilde{e}_{\mathcal{S}}=e_{\mathcal{S}}$, and (iii) $\widetilde{e}_{\mathcal{A}}=e_{\mathcal{A}}$; the invariant $\widetilde{\mathrm{I}}$ and the sets of initial and final states $\widetilde{\mathrm{E}}_{\alpha}$, with $\alpha\in\{0,F\}$, are built similarly, thus, if I is bounded, $\widetilde{\mathrm{I}}$ is bounded as well;
- the evolution function $\widetilde{\mathsf{evl}}$ uses the transformation matrix $\widetilde{\mathsf{A}}$, while both the actuator matrix and the offset vector are those of the CPS $\mathcal{M}$;
- the measurement function $\widetilde{\mathsf{msr}}$ uses the sensor matrix $\widetilde{\mathrm{C}}\triangleq\mathrm{C}\cdot\mathsf{P}$, where C is the sensor matrix of the CPS $\mathcal{M}$, while the error polyhedron is inherited from $\mathcal{M}$ without modifications.

To conclude the proof, we need to show that $\widetilde{\mathcal{M}}$ is equivalent to $\mathcal{M}$. In order to do so, one can observe that the bijective mapping $(c,e)\mapsto(c,\widetilde{e})$ between state of the dynamics graphs $\mathcal{G}_{\mathcal{M}}$ and $\mathcal{G}_{\widetilde{\mathcal{M}}}$ allows to map paths of $\mathcal{G}_{\mathcal{M}}$ into paths of $\mathcal{G}_{\widetilde{\mathcal{M}}}$ and, *vice versa*, where (i) $\widetilde{e}_{\mathcal{X}}=\mathsf{P}^{-1}\cdot e_{\mathcal{X}}$, (ii) $\widetilde{e}_{\mathcal{S}}=e_{\mathcal{S}}$, and (iii) $\widetilde{e}_{\mathcal{A}}=e_{\mathcal{A}}$. The easy step-by-step verification is left to the reader. □

An easy induction on the difference $n_{\mathcal{X}}-(i+j)$ between the dimension and the sum of the two indexes of a i,j-zero-padded matrix allows to show that we can always put a system in a kind of *normal-form* where the transformation matrix has the shape $\mathsf{A}\triangleq\left(\begin{array}{c|c}\Gamma & \Delta\\ \hline \mathbf{0} & \Lambda\end{array}\right)$, where Γ is invertible, Λ is nilpotent, and Δ is an arbitrary matrix. This is formally stated in the following corollary. Observe that all relevant properties or the original transformation

matrix are preserved during the *normalization process*. Finally, it is not hard to see that the computational resources required by this process are polynomially bounded by the dimension of the matrix. Indeed, to perform such a transformation, we need to apply Theorem 1 at most $n_{\mathcal{X}}$ times. The cost of each application is proportional to the sum of (i) the cost of a Gaussian elimination to obtain the transformation matrix $\widetilde{\mathsf{A}}$ and (ii) the cost of the linear transformations of the sensor matrix C together with that of the polyhedra constituting the invariant I and the sets of initial and final states M_I and M_F.

Corollary 1 (CPS Normalization). *For every (rational, bounded, h, k-periodic) CPS $\mathcal{M}$ on $n_{\mathcal{X}}$ variables, there exists an equivalent $i, (n_{\mathcal{X}} - i)$-zero padded (rational, bounded, h, k-periodic) CPS $\widetilde{\mathcal{M}}$, for some $0 \leq i \leq n_{\mathcal{X}}$. Moreover, $\widetilde{\mathcal{M}}$ can be computed from $\mathcal{M}$ in polynomial time.*

As an instance of the CPS normalization process, consider again the CPS $\mathcal{M}_{WT}$ of the water-tank plant described above. It is not hard to see that its transformation matrix A, being 3, 0-zero padded, can be decomposed as follows, where both matrices Δ and Λ are empty (the decimal values previously reported are represented here as fractions):

$$\mathsf{A} = \left(\begin{array}{cccc} 0 & 0 & 3/2 & 3/2 \\ 3/4 & 0 & 0 & -1/2 \\ 1/4 & 1/4 & 0 & 0 \\ \hline 0 & 3/4 & -1/2 & 0 \end{array}\right) = \left(\begin{array}{c|c} \Xi & \Xi \cdot \mu_c \\ \hline \mu_r^{\mathsf{T}} \cdot \Xi & \mu_r^{\mathsf{T}} \cdot \Xi \cdot \mu_c \end{array}\right),$$

where $\mu_r^{\mathsf{T}} = (-1/3, -1, 3)$, and $\mu_c^{\mathsf{T}} = (-2/3, 2/3, 1)$.

At this point, after the application of the normalization process described in the proof of Lemma 1, we obtain the following modified 3, 1-zero-padded 0, 3-periodic transformation matrix $\widetilde{\mathsf{A}}$:

$$\widetilde{\mathsf{A}} = \left(\begin{array}{cccc} -1/2 & -3/2 & 6 & 3/2 \\ 11/12 & 1/2 & -3/2 & -1/2 \\ 1/4 & 1/4 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right) = \left(\begin{array}{c|c} \widetilde{\Gamma} & \widetilde{\Delta} \\ \hline \mathbf{0} & \widetilde{\Lambda} \end{array}\right),$$

$$\text{with } \widetilde{\Gamma} = \Xi \cdot \begin{pmatrix} 1 + 2/9 & 2/3 & -2 \\ -2/9 & 1 - 2/3 & 2 \\ -1/3 & -1 & 1 + 3 \end{pmatrix}.$$

In addition, the modified sensor matrix $\widetilde{\mathsf{C}}$ is:

$$\widetilde{\mathsf{C}} = \begin{pmatrix} -1/25 & -3/25 & 9/25 & 3/25 \\ 0 & 1/20 & 0 & 0 \\ 0 & 0 & 1/20 & 0 \end{pmatrix} = \mathsf{C} \cdot \mathsf{P},$$

$$\text{where } \mathsf{P} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline -1/3 & -1 & 3 & 1 \end{array}\right).$$

An interested reader can also verify that $\widetilde{\mathsf{A}} = \mathsf{P}^{-1} \cdot \mathsf{A} \cdot \mathsf{P}$. Finally, beside the control states, the invariant I is the Cartesian product of the following interval of values: $[0, 100]$ for the first three variables, $[-200/3, 0]$ for the fourth variable, $[-0.12, 12.12]$ for the first sensor, $[-0.05, 5.05]$ for the other two sensors, $\{0, 0.5, 1\}$ for the first actuator, and $\{0, 1\}$ for the other two actuators. The set of initial and final states are modified similarly. To conclude, observe that the normalized CPS $\widetilde{\mathcal{M}}_{WT}$, although equivalent to the original one $\mathcal{M}_{WT}$, does not preserve the physical meaning of the variable x_4 whose corresponding components of the transformation matrix have been modified.

4 REACHABILITY PROBLEM

We now provide an ExpSpace decidability procedure for the reachability/safety problem of bounded periodic CPSs, which is based on the notion of reachability polyhedric quotient. We prove that the same procedure runs in PSpace under the assumption that the condition polyhedra, the invariant, and both the initial and the final sets of states are *rectangular*, *i.e.*, they can be described by means of linear constraints of the form $x \asymp v$, with $\asymp \in \{<, \leq, >, \geq\}$, x a variable, and $v \in \mathbb{Q}$ a rational number. Finally, we show that, in case the boundedness requirement on the invariant is relaxed, the same problem turns out to be undecidable.

In the following, given a linear CPS $\mathcal{M}$, we shall declare that two states $(c_1, e_1), (c_2, e_2) \in \mathrm{I}$ are *equivalent*, in symbols $(c_1, e_1) \equiv (c_2, e_2)$, if the associated control states are equal and the two sensor states belong to the same condition polyhedron. Formally, $(c_1, e_1) \equiv (c_2, e_2)$ if the following properties hold true: (i) $c_1 = c_2$; (ii) $e_{1\mathcal{S}} \in \mathsf{P}_i$ *iff* $e_{2\mathcal{S}} \in \mathsf{P}_i$, for all indexes $i \in [1, m]$, where P_i is the i-th condition polyhedron as described in Item 1 of Definition 3. Intuitively, two states are equivalent if they cannot be distinguished by the control system.

In the next definition we describe how to quotient the dynamics graph $\mathcal{G}_{\mathcal{M}}$ induced by a bounded CPS $\mathcal{M}$ in such a way that (i) physical states locally behaving in a similar manner are grouped into polyhedra, and (ii) the reachability property is preserved.

Definition 4 (Reachability Quotient). *The* reachability quotient *of a linear CPS $\mathcal{M} = \langle \mathrm{M}, \mathsf{trn}, \mathsf{evl}, \mathsf{msr}, \mathsf{act}, \mathrm{I}, \mathrm{M}_I, \mathrm{M}_F \rangle$ is the graph $\mathcal{G}^{\equiv}_{\mathcal{M}} \triangleq \langle \mathrm{W}, \Rightarrow \rangle$ defined as follows:*

- $\mathrm{W} \triangleq \{\mathrm{Q} \subseteq \mathrm{I} : \exists \mathrm{Q}^{\star} \in (\mathrm{I}/\equiv) \,.\, \mathrm{Q} \subseteq \mathrm{Q}^{\star}\}$;
- $\mathrm{Q}_1 \Rightarrow \mathrm{Q}_2$ iff $\mathrm{Q}_2 \in (\{(c_2, e_2) \in \mathrm{I} : \exists (c_1, e_1) \in \mathrm{Q}_1 \,.\, (c_1, e_1) \rightarrow (c_2, e_2)\}/\equiv)$, *for all* $\mathrm{Q}_1, \mathrm{Q}_2 \in \mathrm{W}$.

The sets of elements $\mathrm{Q} \in \mathrm{W}$ *are called* pseudo states. *Moreover,* Q *is* initial *(*resp., final*) if* $\mathrm{Q} \subseteq \mathrm{M}_I$ *(*resp., $\mathrm{Q} \cap \mathrm{M}_F \neq \emptyset$*).*

Intuitively, a pseudo state Q_2 is a successor of a pseudo state Q_1 if every state $(c_2, e_2) \in \mathrm{Q}_2$ is a successor of some state $(c_1, e_1) \in \mathrm{Q}_1$.

The next result shows that the quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ associated with a linear CPS $\mathcal{M}$ preserves the reachability property. To prove this, one can transform a path ρ of $\mathcal{G}_{\mathcal{M}}$ into a path $\rho^{\equiv}$ of $\mathcal{G}^{\equiv}_{\mathcal{M}}$ and *vice versa*, in such a way that the last element of ρ is final *iff* the corresponding element of $\rho^{\equiv}$ is final as well. This can be done, for the forward direction, by replacing each state (c_i, e_i) in ρ with a pseudo state Q_i, following the increasing order of the indexes $i \in \mathbb{N}$, where Q_i is a suitably chosen subset of the equivalence class $[(c_i, e_i)]_{\equiv}$. For the backward direction, in decreasing order of indexes, one extract from each Q_i a representative state $(c_i, e_i) \in \mathrm{Q}_i$ that also preserves the transition relation *w.r.t.* the already chosen state (c_{i+1}, e_{i+1}).

Lemma 2 (Reachability Quotient I). *A dynamics graph $\mathcal{G}_{\mathcal{M}}$ of a CPS $\mathcal{M}$ admits a path starting in an initial state and terminating in a final one* iff *there exists a path in the reachability quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ from an initial pseudo state to a final one.*

Proof. Given a path $\rho = (c_0, e_0), (c_1, e_1), \ldots, (c_k, e_k)$ in $\mathcal{G}_{\mathcal{M}}$ starting from an initial state (c_0, e_0), we can construct a path $\rho^{\equiv} = \mathrm{Q}_0, \mathrm{Q}_1, \ldots, \mathrm{Q}_k$ in the associated reachability quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ as follows, where $[(c, e)]_{\equiv}$ denotes the equivalence class in I containing the state $(c, e) \in \mathrm{I}$:

- $\mathrm{Q}_0 \triangleq [(c_0, e_0)]_{\equiv} \cap \mathrm{M}_I$;
- $\mathrm{Q}_{i+1} \triangleq [(c_{i+1}, e_{i+1})]_{\equiv} \cap \{(c^\star, e^\star) \in \mathrm{I} : (c_i, e_i) \rightarrow (c^\star, e^\star)\}$, for all indexes $0 \leq i < k$.

Obviously, Q_0 is an initial pseudo state and, if (c_k, e_k) is a final state, then Q_k is a final pseudo state.

Dually, given a path $\rho^{\equiv}$ in $\mathcal{G}^{\equiv}_{\mathcal{M}}$ ending in a final pseudo state, we can extract from it several paths ρ of $\mathcal{G}_{\mathcal{M}}$ as follows:

- $(c_k, e_k) \in \mathrm{Q}_k \cap \mathrm{M}_F$;
- $(c_{i-1}, e_{i-1}) \in \{(c^\star, e^\star) \in \mathrm{Q}_{i-1} : (c^\star, e^\star) \rightarrow (c_i, e_i)\}$, for all indexes $0 < i \leq k$.

Obviously, (c_k, e_k) is a final state and, if Q_0 is an initial pseudo state, then (c_0, e_0) is an initial state.

The soundness of the above constructions is easy to prove by standard induction on the length k of the paths. □

By exploiting elementary linear algebra and standard theory of convex polyhedra, one can easily show that every pseudo state along a path in the reachability quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ of a CPS $\mathcal{M}$ can be decomposed into a Cartesian product of control states, polyhedra on variable and sensor states, and actuator states (see Lemma 3).

From now on, by $\mathrm{Y}_1, \ldots, \mathrm{Y}_m \subseteq \mathbb{R}^{n_{\mathcal{X}}}$, we denote the $m \in \mathbb{N}$ polyhedra on variable states such that $\mathrm{P}_i = \mathrm{C} \cdot \mathrm{Y}_i + \mathrm{D}$, for all $i \in [1, m]$, where $\mathrm{P}_i \subseteq \mathbb{R}^{n_{\mathcal{S}}}$ are the condition polyhedra described at Item 1 of Definition 3. In addition, given a polyhedron of variable and sensor states $\mathrm{U} \subseteq \mathbb{R}^{n_{\mathcal{X}}+n_{\mathcal{S}}}$, with $\mathrm{U}{\restriction}\mathcal{X} \subseteq \mathbb{R}^{n_{\mathcal{X}}}$ (*resp.*, $\mathrm{U}{\restriction}\mathcal{S} \subseteq \mathbb{R}^{n_{\mathcal{S}}}$) we indicate the polyhedron of variable (*resp.*, sensor) states only, obtained from U by projecting out the sensor (*resp.*, variable) state components of each vector in U. Observe that $\mathrm{U}{\restriction}\mathcal{X} \subseteq \mathrm{Y}_i$ *iff* $\mathrm{U}{\restriction}\mathcal{S} \subseteq \mathrm{P}_i$, for all $i \in [1, m]$.

Lemma 3 (Reachability Quotient II). *Let $\rho^{\equiv} = \mathrm{Q}_0, \mathrm{Q}_1, \ldots, \mathrm{Q}_k$ be a path in the reachability quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ of a CPS $\mathcal{M}$, with Q_0 initial. Then, for all indexes $i \in [0, k]$, there exist a control state $c_i \in \mathrm{C}$, a polyhedron of variable and sensor states $\mathrm{U}_i \subseteq \mathbb{R}^{n_{\mathcal{X}}+n_{\mathcal{S}}}$, and an actuator state $e_{\mathcal{A}i} \in \mathbb{R}^{n_{\mathcal{A}}}$ such that $\mathrm{Q}_i = \{c_i\} \times \mathrm{U}_i \times \{e_{\mathcal{A}i}\}$. Moreover, for $\mathrm{V}_i \triangleq \mathrm{U}_i{\restriction}\mathcal{X}$, it holds that $\mathrm{V}_{i+1} = (\mathrm{A} \cdot \mathrm{V}_i + \mathrm{B} \cdot e_{\mathcal{A}i+1} + \mathrm{w}) \cap \mathrm{Y}_{j_{i+1}}$, for some index $j_{i+1} \in [1, m]$.*

Proof. First observe that, for all indexes $i \in [0, k]$ and states $(c_{1i}, e_{1i}), (c_{2i}, e_{2i}) \in \mathrm{Q}_i$, it holds that $c_{1i} = c_{2i}$, since $(c_{1i}, e_{1i}) \equiv (c_{2i}, e_{2i})$. Thus, $e_{1i\mathcal{A}} = \mathrm{act}(c_{1i}) = \mathrm{act}(c_{2i}) = e_{2i\mathcal{A}}$. Consequently, $\mathrm{Q}_i = \{c_i\} \times \mathrm{U}_i \times \{e_{\mathcal{A}i}\}$, for some set of variable and sensor states $\mathrm{U}_i \subseteq \mathbb{R}^{n_{\mathcal{X}}+n_{\mathcal{S}}}$, where $c_i = c_{1i} = c_{2i}$ and $e_{\mathcal{A}i} = e_{1i\mathcal{A}} = e_{2i\mathcal{A}}$. Moreover, again by definition of the equivalence relation $\equiv$ among states, it follows that $\mathrm{U}_i \subseteq \mathbb{R}^{n_{\mathcal{X}}} \times \mathrm{P}_{j_i}$, for some index $j_i \in [1, m]$, where P_{j_i} is one of the condition polyhedra. Therefore, $\mathrm{V}_i \subseteq \mathrm{Y}_{j_i}$, where $\mathrm{V}_i \triangleq \mathrm{U}_i{\restriction}\mathcal{X}$. We can now show that U_i is actually a polyhedron. The proof of this fact proceeds by induction on the length k of the path $\rho^{\equiv}$ reaching a certain pseudo state Q_k.

For the base case $k = 0$, we have that $\{c_0\} \times \mathrm{U}_0 \times \{e_{0\mathcal{A}}\} = \mathrm{Q}_0 \subseteq \mathrm{M}_I = \mathrm{C}_I \times \mathrm{F}_I \times \mathrm{G}_I$, since Q_0 is an initial pseudo state, where C_I, F_I, and G_I are the sets described at Item 5 of Definition 3. Therefore, $\mathrm{Q}_0 \in ((\mathrm{C}_I \times \mathrm{F}_I \times \mathrm{G}_I)/\equiv)$, which means that $\mathrm{U}_0 = \mathrm{F}_I \cap (\mathbb{R}^{n_{\mathcal{X}}} \times \mathrm{P}_{j_0})$. However, the Cartesian product of a polyhedron P_{j_0} with $\mathbb{R}^{n_{\mathcal{X}}}$ is a polyhedron and the intersection of two polyhedra is a polyhedron as well. Hence, the thesis holds for Q_0.

As the inductive case $k > 0$, suppose that the property holds true at index $k-1$ and let us show that the same holds for index k. Since $\mathrm{Q}_{k-1} \Rightarrow \mathrm{Q}_k$, by definitions of reachability quotient and graphs of dynamics, we have that, for each state $(c_k, e_k) \in \mathrm{Q}_k$, there exists a state $(c_{k-1}, e_{k-1}) \in \mathrm{Q}_{k-1}$ such that $(c_{k-1}, e_{k-1}) \rightarrow (c_k, e_k)$. This means that $e_{k\mathcal{X}} = \mathrm{A} \cdot e_{k-1\mathcal{X}} + \mathrm{B} \cdot e_{k\mathcal{A}} + \mathrm{w}$, from which it follows that $\mathrm{V}_k = (\mathrm{A} \cdot \mathrm{V}_{k-1} + \mathrm{B} \cdot e_{\mathcal{A}k} + \mathrm{w}) \cap \mathrm{Y}_{j_k}$. Now, by inductive hypothesis, Q_{k-1} is a polyhedron. Thus V_{k-1} is a polyhedron as well, implying that V_k satisfies the same property being obtained from the first via a linear transformation and an intersection. Moreover, by Item 3 of Definition 3, we necessarily have $\mathrm{Q}_k{\restriction}\mathcal{S} = \mathrm{C} \cdot \mathrm{V}_k + \mathrm{D}$. Hence, this set is a polyhedron too. Consequently, Q_k enjoys the required property, concluding the proof. □

We now provide a proposition describing the structure of an arbitrary power of an i, j-zero-padded matrix. The easy proof is by mathematical induction on the power index.

Proposition 1 (Zero-Padded Power). *The k-th power of an i, j-zero-padded matrix A of dimension $n \in \mathbb{N}_+$ and index $\ell \in \mathbb{N}_+$, where $\ell \leq k \in \mathbb{N}$, is equal to*

$$\mathrm{A}^k = \left(\begin{array}{c|c} \Gamma^k & \Delta^\star \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right), \text{ with } \mathrm{A} = \left(\begin{array}{c|c} \Gamma & \Delta \\ \hline \mathbf{0} & \Lambda \end{array}\right),$$

for some matrix $\Delta^\star \in \mathbb{R}^{(n-j)\times j}$.

Finally, everything is in place to provide our ExpSpace decidability procedure for the reachability problem of rational bounded h, k-periodic CPSs. In addition, we prove that the same procedure runs in PSpace under the assumption that the condition polyhedra, the invariant, and both the initial and final sets of states are rectangular, *i.e.*, they can be described by means of linear constraints of the form $x \asymp v$, with $\asymp \in \{<, \leq, >, \geq\}$, x a variable, and $v \in \mathbb{Q}$ a rational number. In such a case, we call the CPS *rectangular*. Notice that the CPS of the example described in the previous section is rectangular.

Thanks to Lemma 2, one can solve the problem for a CPS $\mathcal{M}$ by reducing it to a nondeterministic search in the reachability quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ for a path $\rho^{\equiv} = \mathrm{Q}_0, \mathrm{Q}_1, \ldots, \mathrm{Q}_k$ meeting a final pseudo state Q_k and starting from an initial one Q_0. In particular, the search does not require the construction of the entire structure $\mathcal{G}^{\equiv}_{\mathcal{M}}$ in advance, since every pseudo state Q_{i+1} along $\rho^{\equiv}$ can be computed directly from the previous one Q_i, as described by Lemma 3, via the equality

$$\mathrm{V}_{i+1} = (\mathrm{A} \cdot \mathrm{V}_i + \mathrm{B} \cdot e_{\mathcal{A}i+1} + \mathrm{w}) \cap \mathrm{Y}_{j_{i+1}}.$$

Moreover, in general, there are at most doubly-exponentially many reachable pseudo states, since there are at most doubly-exponentially many polyhedra that can reside entirely in the invariant of the system, as we shall show later in this section. Indeed, a convex polyhedron can be uniquely identified by its set of vertex and there are at most exponentially many suitably such vertexes. In the case of rectangular constraints, instead, we are able to show that the number of rectangular polyhedra that can be reached is at most

exponential. This is because, to identify a single rectangle, it is enough to determine the coordinate of $n_{\mathcal{X}}$ of its vertexes, where $n_{\mathcal{X}}$ is the dimension of the variable state space.

The decision procedure we provide strongly relies on the zero-padded normal form of the transformation matrix A of $\mathcal{M}$ ensured by Corollary 1. With more detail, such a property induces in its turn a normal form on the variable-state polyhedra $\mathsf{V}_i \subseteq \mathbb{R}^{n_{\mathcal{X}}}$. Indeed, it can be shown that, if A is h, k-periodic, after a transient of length h, each set V_{i+h+1} satisfies the equality

$$\mathsf{V}_{i+h+1} = (\mathsf{A}^i \cdot \mathsf{V}_{h+1}) \cap \bigcap_{j=0}^{h+k} \mathsf{A}^j \cdot \mathsf{Z}^\star_{i,j} + z^\star_i,$$

where $\mathsf{Z}^\star_{i,j}$ is a polyhedron (*resp.*, rectangular polyhedron) among doubly-exponentially (*resp.*, exponentially) many polyhedra (*resp.*, rectangular polyhedra) that are independent from V_{h+1} and only depend on the invariant I and the condition polyhedra $\mathsf{P}_1, \ldots, \mathsf{P}_m$. Moreover, there are only exponentially many displacements $z^\star_i$ Now, thanks to Proposition 1, one can observe that $\mathsf{A}^i \cdot \mathsf{V}_{h+1} = \mathsf{A}^{i+k} \cdot \mathsf{V}_{h+1}$. Thus, the number of possible reachable pseudo states Q_i is linear in the number of the sets $\mathsf{Z}^\star_{i,j}$ and vectors $z^\star_i$. This shall conclude the proof.

Theorem 2 (Decidability). *The reachability problem for a rational bounded h, k-periodic CPS can be decided in ExpSpace. If the above CPS is also rectangular, then the reachability problem can be decided in PSpace.*

Proof. By an application of Corollary 1, the reachability problem for an arbitrary rational bounded h, k-periodic CPS on $n_{\mathcal{X}}$ variables can be linearly reduced to the same problem for a rational bounded h, k-periodic $p, (n_{\mathcal{X}} - p)$-zero-padded CPS $\mathcal{M}$, for some $0 \leq p \leq n_{\mathcal{X}}$. The latter can then be solved, due to Lemmas 2 and 3, by nondeterministically searching in the associated reachability quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ for a path $\rho^{\equiv} = \mathsf{Q}_0, \ldots, \mathsf{Q}_n$ that starts in an initial pseudo state Q_0 and ends in a final one Q_n. Since such a search does not require the construction of the entire quotient $\mathcal{G}^{\equiv}_{\mathcal{M}}$ and every pseudo state Q_{i+1} can be computed from the previous one Q_i by using the decomposition described in the statement of Lemma 3, it shall be sufficient to employ a counter to verify if a loop has been found before encountering a final pseudo state. Such a counter has exponentially many bits in case we are considering arbitrary polyhedra, while only polynomially many, if we focus on rectangular constraints. The required complexity follows directly from this simple observation.

Let us proceed with the details of the proof. First notice that, by Lemma 3, there is a bijection between a path $\mathsf{Q}_0, \ldots, \mathsf{Q}_n$ and a sequence $(c_0, \mathsf{V}_0), \ldots, (c_n, \mathsf{V}_n)$ of the same length, where $\mathsf{V}_{i+1} = (\mathsf{A} \cdot \mathsf{V}_i + \mathsf{B} \cdot e_{\mathcal{A}i+1} + \mathsf{w}) \cap \mathsf{Y}_{j_{i+1}}$ and $e_{\mathcal{A}i} = \mathsf{act}(c_i)$, for some index $j_{i+1} \in [1, m]$. The proof consists in showing the following sequence of five claims, whose proofs can be found in the Appendix, where we set (i) $\mathsf{w}_i \triangleq \mathsf{B} \cdot e_{\mathcal{A}i} + \mathsf{w}$, (ii) $z_i \triangleq \sum_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{w}_l$, and (iii) $\mathsf{Z}_i \triangleq \mathsf{Y}_{j_i} - z_i$.

The first claim states that every polyhedra V_i reachable during the search is completely included into a polyhedron computable directly from the initial one V_0.

Claim 1. $\mathsf{V}_i \subseteq (\mathsf{A}^i \cdot \mathsf{V}_0) \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l + z_i$, *for all* $i \in \mathbb{N}$.

Thanks to the above inequality, we can show that all components from the $(i+1)$-th to the $n_{\mathcal{X}}$-th of a vector in the polyhedron V_{h+1}, obtained after the transient has terminated, are constant.

Claim 2. $(e_{\mathcal{X}1})_j = (e_{\mathcal{X}2})_j$, *for all vectors* $e_{\mathcal{X}1}, e_{\mathcal{X}2} \in \mathsf{V}_{h+1}$ *and indexes* $i + 1 \leq j \leq n_{\mathcal{X}}$.

After the transient phase is concluded, all reachable polyhedra have a more structured form than those reached before, as described in the statement of the following claim, where we set:

- $z^\star_i \triangleq \sum_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{w}_{l+h+1}$;
- $\mathsf{Z}^\star_i \triangleq \{e_{\mathcal{X}} \in \mathsf{Y}_{j_{i+h+1}} : \forall p{+}1 \leq j \leq n_{\mathcal{X}} \,.\, (e_{\mathcal{X}})_j = (z^\star_{i+h+1})_j\} - z^\star_i$.

Claim 3. $\mathsf{V}_{i+h+1} = \mathsf{A}^i \cdot (\mathsf{V}_{h+1} \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}^\star_l) + z^\star_i$, *for all* $i \in \mathbb{N}$.

At this point, we are able to describe a normal form for all polyhedra that are reachable after the transient phase is concluded, where we set $\mathsf{Z}^\star_{i,j} \triangleq \mathsf{Z}^\star_{i-j}$, if $i - j \leq h$, and $\mathsf{Z}^\star_{i,j} \triangleq \bigcap_{\substack{q \in [0,\, k[\\ i-j = l + q \cdot k}} \mathsf{Z}^\star_l$, otherwise.

Claim 4. $\mathsf{V}_{i+h+1} = (\mathsf{A}^i \cdot \mathsf{V}_{h+1}) \cap \bigcap_{j=0}^{h+k} \mathsf{A}^j \cdot \mathsf{Z}^\star_{i,j} + z^\star_i$, *for all* $i \in \mathbb{N}$.

Finally, we can give a bound on the number of reachable polyhedra V_i during the nondeterministic search for a final one.

Claim 5. *There are doubly-exponentially (*resp.*, exponentially) many polyhedra (*resp.*, rectangular polyhedra)* $\mathsf{Z}^\star_{i,j}$.

To conclude the proof, it is enough to observe that, thanks to Claims 4 and 5, in order to maintain a polyhedron V_{i+h+1} along the search, after the transient phase is terminated, it is enough to record at every step the index i, the $k + h + 1$ polyhedra $\mathsf{Z}^\star_{i,j}$, and the vector $z^\star_i$. Hence, the complexity immediately follows. □

It is quite easy to prove that, if the system invariant is not bounded, then the decidability result does not hold anymore. Indeed, such systems can simulate a standard two-counter machine [12, 19], where the associated control logic is embedded in the controller and the two counters are maintained by the environment into two physical variables. We prove the undecidability result for rational unbounded h, k-periodic *rectangular* CPSs, the generalization to non-rectangular CPSs is an immediate consequence.

Theorem 3 (Undecidability). *The reachability problem of rational unbounded h, k-periodic rectangular CPSs is undecidable.*

Proof. To prove the undecidability of the reachability problem for rational unbounded periodic rectangular CPSs, we describe a reduction from the halting problem of a two-counter machine. First, consider a rational unbounded 0, 1-periodic CPS with two variables, two sensors, and two actuators defined as follows: $\mathcal{M} = \langle \mathsf{C} \times \mathbb{R}^2, \mathsf{trn}, \mathsf{evl}, \mathsf{msr}, \mathsf{act}, \mathsf{C} \times \mathbb{R}^2, \{(c_0, (0,0))\}, \mathsf{M}_F \rangle$; the transformation, sensor, and actuator matrices are the identity, *i.e.*, $\mathsf{A} = \mathsf{C} = \mathsf{B} = \mathsf{I}$; the offset vector is the zero one, *i.e.*, $\mathsf{w} = (0,0)$; the error polyhedron is the trivial one, *i.e.* $\mathsf{D} = \{(0,0)\}$. Now, it is easy to see that the logic of the two-counter machine can be simulated by a cyber controller with the same set of states C and the same initial state c_0 by suitably testing each sensor for zero, where the increment/decrement of the first/second counter is mapped to a $1/-1$ value on the associated actuator. The final states of the controller are the halting states of the machine M_F. Obviously, the invariant, both the initial and

final sets of states, and the the testing of a sensor for zero can be described by means of rectangular linear constraints. Hence $\mathcal{M}$ is rectangular. At this point, it is immediate to observe that the solution of the reachability problem on the described CPS would correspond to a solution of the halting problem of the two-counter machine. The undecidability result immediately follows. □

Corollary 2. *The reachability problem of rational unbounded h, k-periodic CPSs is undecidable.*

5 CONCLUSIONS, RELATED AND FUTURE WORK

The paper provides a decidability procedure of the *reachability/safety problem* for a significant subclass of discrete-time linear CPSs, more precisely, for h, k-periodic CPSs, *i.e.*, CPSs whose physical process in isolation, *i.e.*, without any interaction with the controller, has a behavior with a period k and transient h. A necessary requirement for decidability is the boundedness of the invariant: if the invariant is not bound, indeed, the reachability problem of h, k-periodic CPSs is still undecidable, even under the hypotheses of rectangular constraints.

The steps followed to derive the decidability result are as follows. The first step of our reachability result consists in providing a polynomial-time transformation of our CPSs in its corresponding zero-padded normal form. One of the main technical challenges of the paper, in fact, consists in proving that, for every bounded periodic CPS, there exists a corresponding equivalent zero-padded normal form (Lemma 1, Theorem 1, and Corollary 1). This result is not a trivial one, because it requires something similar to a partial matrix diagonalization process on the rational field $\mathbb{Q}$. Then, we describe a ExpSpace (*resp.*, PSpace) decidability procedure of the *reachability/safety problem* for bounded periodic (*resp.*, rectangular) CPSs, which is based on the notion of reachability quotient (Theorem 2). Intuitively, we show that if there exists an execution of the CPS starting from an initial state that reaches a final one, there exists a corresponding path in the reachability quotient and *vice versa*. In other words, we describe how to quotient a bounded periodic CPS in such a way that (i) physical states locally behaving in a similar way are grouped into polyhedra, and (ii) the reachability property is preserved. In the general case, we show that there are at most doubly-exponentially many polyhedra that can be entirely contained in our bounded system invariants. This because every polyhedron can be uniquely identified by its set of vertexes and there are at most exponentially many values to associate with them inside the invariant. However, in the case of rectangular CPSs, we are able to prove that the number of possible rectangular polyhedra with the same property is at most exponential in the number of physical state variables, since every rectangular polyhedron only requires a number of points equal to the dimension of the space to be identified. Notice that a PSpace lower bound should be easily derivable from the emptiness problem of classic timed automata, since these are basically periodic CPSs in which the transformation matrix is the identity and where the boundedness of the invariant is somehow intrinsic in the nature of the problem (it can be computed from the maximal constant occurring in a clock constraint).

Finally, we show that, in case the boundedness requirement on the system invariant is not satisfied, the same problem turns out to be undecidable, even when assuming rectangular constraints (Theorem 3), since such systems can simulate a standard two-counter machine [12, 19].

Related work. The reachability problem for hybrid automata has been shown to be decidable for a number of classes of hybrid automata including *timed automata* [4], certain subclasses of *rectangular hybrid automata* [8], *semi-algebraic o-minimal hybrid automata* [11], *semi-algebraic STORMED hybrid systems* [28], and, more recently, *initialized linear inclusion automata* [24].

In the last three classes of automata mentioned above the dynamics of the state variables is given by an exponential function. However, in general, reachability remains undecidable even for simpler classes, with simpler dynamics, such as *linear hybrid automata* [5], in which the dynamics of the variables are defined by linear differential inequalities.

Nevertheless, besides the papers [4, 8], decidability has been proven for a number of subclasses of linear hybrid automata equipped with either continuous or discrete time. In the continuous case, decidability has been proven for: (i) *planar linear hybrid automata* [22], a subclass with only two state variables, monotonic along some direction in the plane and with no resets; (ii) *rectangular hybrid automata*, with continuous state variables, but controllers that check them in discrete-time instants [7]; (iii) *initialized rectangular automata* [23], in which the bounds of the derivative of each variable are constants except when the variable assumes an integer value or it is initialized to a new value.

In the discrete case, decidability has been proven for *lazy rectangular automata* [1], in which the observation of the continuous space takes place with bounded delays; basically, this is a generalization of [7], where the discrete time behavior of rectangular automata is studied under the condition that all instantaneous transitions should take place only at integer-valued instances of time. This work was subsequently extended [2, 9] with the introduction of two key features: (i) the values of the continuous variables can be observed with only finite precision, (ii) the guards controlling the transitions are finite conjunctions of arbitrary linear constraints.

Another significant achievement in discrete-time linear hybrid systems can be found in the *control-theory* paper [27]. In that paper, the dynamics of a physical system is given by means of a discrete-time evolution law of the form

$$x_{k+1} = \mathrm{A}x_k + \mathrm{B}u_k + \mathrm{C}d_k$$

in which x_k is the current *state vector*, u_k is the *input vector* (*i.e.*, the control actions implemented through actuators), and d_k denotes the vector of *disturbance variables*; A, B and C are rational matrices characterizing the dynamics of the system. The paper proves that (a control-theory problem corresponding to) reachability is decidable under the following hypotheses: (i) the matrix resulting from the calculation $\mathrm{B}(\mathrm{AB})\ldots(\mathrm{A}^{n-1}\mathrm{B})$ has maximum rank; (ii) for any disturbance d, it must hold $\mathrm{M}((\mathrm{A}^{n-1}\mathrm{C})\ldots\mathrm{C})d^n \leq \beta$, where M and β come from the safe set constraint $\mathrm{M}x \leq \beta$, for any state vector x.

Linear control systems, a class of control systems closely related to the previous ones, even supports decidable model checking of Linear Temporal Logic (LTL) formula [25, 26].

Finally, in order to get around the limitations of the automatic verification of linear hybrid systems, the paper [6] provides a semi-decision method for the safety of *robust polynomial hybrid system*, a class of continuous polynomial hybrid systems enriched with a simple model of *perturbation* (or noise). Intuitively, all physical variables of these systems are subject to a perturbation that is at most ϵ, for some fixed $\epsilon > 0$. The decidability holds when assuming certain distances, such as Euclidean distance, between genuine and perturbed physical values, but not for others, such as discrete metrics or radar-screen metrics. As reported by the author himself, the model of perturbation used in the paper is actually a bit too simplistic: realistic models of noise should better be quantitative, representing noise in terms of some appropriate probabilistic distribution. The paper does not provide any computation of the complexity of the proposed methodology.

Future work. We would like to investigate new significant subclasses of linear CPSs, with possibly more efficient decidability procedures. In particular, it would be interesting to understand how to relax the linearity and periodicity constraints still maintaining a decidable reachability problem.

This paper is part of a wider project whose goal is to apply formal methods to lay and streamline logical foundations to reason about CPSs [21] (see [13, 18]) and *cyber-physical attacks* [29], *i.e.*, security breaches in cyberspace that adversely affect the physical processes of CPSs (see [15–17]). Actually, we will consider applying the results of the current paper in the context of *CPS security* [29] by developing a *ad hoc* logics for building up a security analysis to statically detect cyber-physical attacks targeting both physical devices and logical components (a first attempt in this direction can be found in [14]).

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their valuable comments. The second author has been partially supported by the project "Dipartimenti di Eccellenza 2018 −2022" funded by the Italian Ministry of Education, Universities and Research (MIUR). The third author acknowledges the support of the GNCS 2018 project "Metodi Formali per la Verica e la Sintesi di Sistemi Discreti e Ibridi".

REFERENCES

[1] Manindr Agrawal and P. S. Thiagarajan. 2004. Lazy Rectangular Hybrid Automata. In *Proceedings of the 7th. International Workshop on Hybrid Systems: Computation and Control (HSCC'04) (Lecture Notes in Computer Science)*, Vol. 2993. Springer, 1–15. https://doi.org/10.1007/b96398

[2] Manindr Agrawal and P. S. Thiagarajan. 2005. The Discrete Time Behavior of Lazy Linear Hybrid Automata. In *Proceedings of the 8th. International Workshop on Hybrid Systems: Computation and Control (HSCC'05) (Lecture Notes in Computer Science)*, Vol. 3414. Springer, 55–69. https://doi.org/10.1007/978-3-540-31954-2_4

[3] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and Sergio Yovine. 1995. The Algorithmic Analysis of Hybrid Systems. *Theor. Comput. Sci.* 138, 1 (1995), 3–34. https://doi.org/10.1016/0304-3975(94)00202-T

[4] Rajeev Alur and David L. Dill. 1994. A Theory of Timed Automata. *Theor. Comput. Sci.* 126, 2 (1994), 183 – 235. https://doi.org/10.1016/0304-3975(94)90010-8

[5] Rajeev Alur, Thomas A. Henzinger, and Pei-Hsin Ho. 1996. Automatic Symbolic Verification of Embedded Systems. *IEEE Trans. Software Eng.* 22, 3 (1996), 181–201. https://doi.org/10.1109/32.489079

[6] Martin Fränzle. 1999. Analysis of Hybrid Systems: An Ounce of Realism Can Save an Infinity of States. In *Proceedings of the 13th. International Workshop on Computer Science Logic (CSL'99) (Lecture Notes in Computer Science)*, Vol. 1683. Springer, 126–140. https://doi.org/10.1007/3-540-48168-0

[7] Thomas A. Henzinger and Peter W. Kopke. 1999. Discrete-Time Control for Rectangular Hybrid Automata. *Theor. Comput. Sci.* 221, 1 (1999), 369 – 392. https://doi.org/10.1016/S0304-3975(99)00038-9

[8] Thomas A. Henzinger, Peter W. Kopke, Anuj Puri, and Pravin Varaiya. 1998. What's Decidable about Hybrid Automata? *J. Comput. System Sci.* 57, 1 (1998), 94 – 124. https://doi.org/10.1006/jcss.1998.1581

[9] Susmit Jha, Bryan A. Brady, and Sanjit A. Seshia. 2007. Symbolic Reachability Analysis of Lazy Linear Hybrid Automata. In *Proceedings of the 5th. International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'07) (Lecture Notes in Computer Science)*, Vol. 4763. Springer, 241âĂŞ256. https://doi.org/10.1007/978-3-540-75454-1_18

[10] Siddhartha Kumar Khaitan and James D. McCalley. 2015. Design Techniques and Applications of Cyberphysical Systems: A Survey. *IEEE Systems Journal* 9, 2 (2015), 350–365. https://doi.org/10.1109/JSYST.2014.2322503

[11] Gerardo Lafferriere, George J. Pappas, and Shankar Sastry. 2000. O-Minimal Hybrid Sstems. *Mathematics of Control, Signals, and Systems* 13, 1 (2000), 1–21. https://doi.org/10.1007/PL00009858

[12] Joachim Lambek. 1961. How to Program an Infinite Abacus. *Canad. Math. Bull.* 4 (1961), 295–302. https://doi.org/10.4153/CMB-1961-032-6

[13] Ruggero Lanotte and Massimo Merro. 2018. A semantic theory of the Internet of Things. *Information and Computation* 259, 1 (2018), 72–101. https://doi.org/10.1016/j.ic.2018.01.001

[14] Ruggero Lanotte, Massimo Merro, and Andrei Munteanu. 2018. A Modest Security Analysis of Cyber-Physical Systems: A Case Study. In *Proceedings of the 38th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE'18) (Lecture Notes in Computer Science)*, Vol. 10854. Springer, 58–78. https://doi.org/10.1007/978-3-319-92612-4

[15] Ruggero Lanotte, Massimo Merro, Andrei Munteanu, and Luca Viganò. 2019. A Formal Approach to Physics-Based Attacks in Cyber-Physical Systems (Exended Version). *CoRR* abs/1902.04572 (2019).

[16] Ruggero Lanotte, Massimo Merro, Riccardo Muradore, and Luca Viganò. 2017. A Formal Approach to Cyber-Physical Attacks. In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*. IEEE Computer Society, 436–450. https://doi.org/10.1109/CSF.2017.12

[17] Ruggero Lanotte, Massimo Merro, and Simone Tini. 2018. Towards a formal notion of impact metric for cyber-physical attacks. In *Proceedings of the 14th International Conference on Integrated Formal Methods (IFM'18) (Lecture Notes in Computer Science)*, Vol. 11023. Springer, 296–315. https://doi.org/10.1007/978-3-319-98938-9

[18] Ruggero Lanotte, Massimo Merro, and Simone Tini. 2019. A Probabilistic Calculus of Cyber-Physical Systems. *Information and Computation* (2019).

[19] Marvin L. Minsky. 1961. Recursive Unsolvability of Post's Problem of "Tag" and other Topics in Theory of Turing Machines. *The Annals of Mathematics* 74, 3 (1961), 437–455.

[20] Ben Noble and James W. Daniel. 1988. *Applied linear algebra*. Prentice Hall.

[21] André Platzer. 2018. *Logical Foundations of Cyber-Physical Systems*. Springer. https://doi.org/10.1007/978-3-319-63588-0

[22] Pavithra Prabhakar, Vladimeros Vladimerou, Mahesh Viswanathan, and Geir E. Dullerud. 2015. A decidable class of planar linear hybrid systems. *Theoretical Computer Science* 574 (2015), 1 – 17. https://doi.org/10.1016/j.tcs.2014.11.018

[23] Anuj Puri and Pravin Varaiya. 1994. Decidability of Hybrid Systems with Rectangular Differential Inclusions. In *Proceedings of the 6th International Conference on Computer Aided Verification (CAV '94) (Lecture Notes in Computer Science)*, Vol. 818. Springer, 95–104. https://doi.org/10.1007/3-540-58179-0_46

[24] Nima Roohi. 2017. *Remedies for building reliable cyber-physical systems*. Ph.D. Dissertation. University of Illinois at Urbana-Champaign.

[25] Paulo Tabuada and George J. Pappas. 2003. Model Checking LTL over Controllable Linear Systems is Decidable. In *Proceedings of the 6th International Workshop on Hybrid Systems: Computation and Control (HSCC'03) (Lecture Notes in Computer Science)*, Vol. 2623. Springer, 498–513. https://doi.org/10.1007/3-540-36580-X_36

[26] Paulo Tabuada and George J. Pappas. 2006. Linear Time Logic Control of Discrete–Time Linear Systems. *IEEE Trans. Automat. Control* 51(12) (2006), 1862–1877. https://doi.org/10.1109/TAC.2006.886494

[27] René Vidal, Shawn Schaffert, Omid Shakernia, John Lygeros, and Shankar Sastry. 2001. Decidable and semi-decidable controller synthesis for classes of discrete time hybrid systems. In *Proceedings of the 40th IEEE Conference on Decision and Control (CDC'01)*, Vol. 2. IEEE Computer Society, 1243–1248. https://doi.org/10.1109/CDC.2001.981057

[28] Vladimeros Vladimerou, Pavithra Prabhakar, Mahesh Viswanathan, and Geir E. Dullerud. 2008. STORMED Hybrid Systems. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP'08) (Lecture Notes in Computer Science)*, Vol. 5126. Springer, 136–147. https://doi.org/10.1007/978-3-540-70583-3_12

[29] Yuriy Zacchia Lun, Alessandro D'Innocenzo, Francesco Smarra, Ivano Malavolta, and Maria Domenica Di Benedetto. 2019. State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software* 149 (2019), 174–216. https://doi.org/10.1016/j.jss.2018.12.006

A DETAILS OF THE PROOF OF THEOREM 2

Claim 1. $\mathsf{V}_i \subseteq \mathsf{A}^i \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l + z_i$, *for all* $i \in \mathbb{N}$.

Proof. The proof proceeds by induction. The base case $i = 0$ is trivial, since $\mathsf{A}^0 = \mathsf{I}$ and, by definition, an empty-indexed intersection contains all elements and an empty-indexes summation assumes zero as value, thus, $\bigcap_{l=1}^{0} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l = \mathbb{R}^{n_\mathcal{X}}$ and $z_0 = 0$. Suppose now that the above inclusion holds at index i and let us prove it for index $i+1$. The steps of our reasoning are reported in the following, where we express the polyhedron V_{i+1} as $(\mathsf{A} \cdot \mathsf{V}_i + \mathsf{w}_{i+1}) \cap \mathsf{Y}_{j_{i+1}}$.

$$\mathsf{V}_{i+1} = (\mathsf{A} \cdot \mathsf{V}_i + \mathsf{w}_{i+1}) \cap \mathsf{Y}_{j_{i+1}} \tag{1}$$

$$\subseteq (\mathsf{A} \cdot (\mathsf{A}^i \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l + z_i) + \mathsf{w}_{i+1}) \cap \mathsf{Y}_{j_{i+1}} \tag{2}$$

$$= (\mathsf{A} \cdot (\mathsf{A}^i \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l) + \mathsf{A} \cdot z_i + \mathsf{w}_{i+1}) \cap \mathsf{Y}_{j_{i+1}} \tag{3}$$

$$= (\mathsf{A} \cdot (\mathsf{A}^i \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l) + z_{i+1}) \cap \mathsf{Y}_{j_{i+1}} \tag{4}$$

$$= \mathsf{A} \cdot (\mathsf{A}^i \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l) \cap (\mathsf{Y}_{j_{i+1}} - z_{i+1}) + z_{i+1} \tag{5}$$

$$= \mathsf{A} \cdot (\mathsf{A}^i \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l) \cap \mathsf{Z}_{i+1} + z_{i+1} \tag{6}$$

$$\subseteq \mathsf{A}^{i+1} \cdot \mathsf{V}_0 \cap \mathsf{A} \cdot \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l \cap \mathsf{Z}_{i+1} + z_{i+1} \tag{7}$$

$$= \mathsf{A}^{i+1} \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{i+1} \mathsf{A}^{i+1-l} \cdot \mathsf{Z}_l + z_{i+1} \tag{8}$$

On Step 1 we have the equality observed above. The inclusion on Step 2 is obtained from Step 1 by applying the inductive hypothesis and the fact that the function $\mathsf{F}(\mathsf{V}) \triangleq (\mathsf{A} \cdot \mathsf{V} + \mathsf{w}_{i+1}) \cap \mathsf{Y}_{j_{i+1}}$ is monotone, *i.e.*, if $\mathsf{V}' \subseteq \mathsf{V}''$ then $\mathsf{F}(\mathsf{V}') \subseteq \mathsf{F}(\mathsf{V}'')$. The third step follows from the second one by distributing the product of A over the sum, while the forth is then due just to the absorption of the term w_{i+1} inside the term z_{i+1}, since $z_{i+1} = \mathsf{A} \cdot z_i + \mathsf{w}_{i+1}$. Step 5 is derived from Step 4 by using the simple equality $(\mathsf{V}+z) \cap \mathsf{Y} = (\mathsf{V} \cap (\mathsf{Y}-z)) + z$. Intuitively, the intersection of two polyhedra, the first of which is translated by a certain vector z, can be obtained by translating the second in the opposite direction $-z$, computing the intersection, and then translating the result by z. Step 6 immediately follows by applying the definition of the polyhedron Z_{i+1}. By applying the inclusion $\mathsf{A} \cdot (\mathsf{V}' \cap \mathsf{V}'') \subseteq \mathsf{A} \cdot \mathsf{V}' \cap \mathsf{A} \cdot \mathsf{V}''$, we derive Step 7 from the previous one. Observe that, the converse does not necessarily hold when A is singular. Finally, in Step 8, we just absorb the polyhedron Z_{i+1} inside the intersection $\bigcap_{l=0}^{i+1} \mathsf{A}^{i+1-l} \cdot \mathsf{Z}_l$. □

Claim 2. $(e_{\mathcal{X}1})_j = (e_{\mathcal{X}2})_j$, *for all vectors* $e_{\mathcal{X}1}, e_{\mathcal{X}2} \in \mathsf{V}_{h+1}$ *and indexes* $i+1 \leq j \leq n_\mathcal{X}$.

Proof. Since A is an h,k-periodic p, $(n_\mathcal{X} - p)$-zero-padded matrix, by Proposition 1, we have that

$$\left(\begin{array}{c|c} \Gamma^{k+h+1} & \Delta^\star \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right) = \mathsf{A}^{k+h+1} = \mathsf{A}^{h+1} = \left(\begin{array}{c|c} \Gamma^{h+1} & \Delta^\star \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right),$$

for some matrix $\Delta^\star \in \mathbb{R}^{p \times (n_\mathcal{X} - p)}$. Therefore, $\Gamma^{k+h+1} = \Gamma^{h+1}$. Moreover, Γ is non-singular, since it has rank p equal to its dimension, so, it admits an inverse Γ^{-1}. Thus, $\Gamma^{k+1} = \Gamma^{-h} \cdot \Gamma^{k+h+1} = \Gamma^{-h} \cdot \Gamma^{h+1} = \Gamma$, *i.e.*, Γ is $0,k$-periodic. In addition, for any set $\mathsf{V} \subseteq \mathbb{R}^{n_\mathcal{X}}$, vector $e_\mathcal{X} \in \mathsf{A}^{h+1} \cdot \mathsf{V}$, and index $p+1 \leq j \leq n_\mathcal{X}$, we have that the j-th component of $e_\mathcal{X}$ is zero, *i.e.*, $(e_\mathcal{X})_j = 0$. This is due to the fact that all rows of A^{h+1} from the $(p+1)$-th to the last one are zero vectors. Consequently, it holds that the components from the $(p+1)$ to $n_\mathcal{X}$ of a vector in V_{h+1} are constant. Formally, $(e_{\mathcal{X}1})_j = (e_{\mathcal{X}2})_j$, for all $e_{\mathcal{X}1}, e_{\mathcal{X}2} \in \mathsf{V}_{h+1}$ and $p+1 \leq j \leq n_\mathcal{X}$. This easily follows from Claim 1 applied to $i = h+1$:

$$\mathsf{V}_{h+1} \subseteq \mathsf{A}^{h+1} \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{h+1} \mathsf{A}^{h+1-l} \cdot \mathsf{Z}_l + z_{h+1}.$$

Indeed, all vectors in $\mathsf{A}^{h+1} \cdot \mathsf{V}_0 \cap \bigcap_{l=1}^{h+1} \mathsf{A}^{h+1-l} \cdot \mathsf{Z}_l$ have zero value on the components from the $(p+1)$-th to the last one, and all of them are translated by the same vector z_{h+1} in order to obtain those in the covering of V_{h+1}. □

Claim 3. $\mathsf{V}_{i+h+1} = \mathsf{A}^i \cdot \mathsf{V}_{h+1} \cap \bigcap_{l=1}^{i} \mathsf{A}^{i-l} \cdot \mathsf{Z}_l^\star + z_i^\star$, *for all* $i \in \mathbb{N}$.

Proof. The proof proceeds by induction on the index i exactly as the one of Claim 1, where, in place of the inclusion $\mathsf{A} \cdot (\mathsf{V}' \cap \mathsf{V}'') \subseteq \mathsf{A} \cdot \mathsf{V}' \cap \mathsf{A} \cdot \mathsf{V}''$ at Step 7, we use the equality $\mathsf{A} \cdot (\mathsf{V}' \cap \mathsf{V}'') = \mathsf{A} \cdot \mathsf{V}' \cap \mathsf{A} \cdot \mathsf{V}''$ that holds true under the assumption that (i) A is p, $(n_\mathcal{X} - p)$-zero-padded and (ii) $(e_{\mathcal{X}1})_j = (e_{\mathcal{X}2})_j$, for all $e_{\mathcal{X}1}, e_{\mathcal{X}2} \in \mathsf{V}' \cup \mathsf{V}''$ and $p+1 \leq j \leq n_\mathcal{X}$, *i.e.*, both V' and V'' are constants on the components from the $(p+1)$-th to the last one. This can be done, thanks to Claim 2, because of the fact that V_{h+1} is constant on the components of its vectors from the $(p+1)$-th to the last one. Indeed, for any vector $e_\mathcal{X} \in \mathsf{A} \cdot \mathsf{V}' \cap \mathsf{A} \cdot \mathsf{V}''$, there exist two vectors $e_\mathcal{X}{}' \in \mathsf{V}'$ and $e_\mathcal{X}{}'' \in \mathsf{V}''$ such that $e_\mathcal{X} = \mathsf{A} \cdot e_\mathcal{X}{}' = \mathsf{A} \cdot e_\mathcal{X}{}''$. Now, consider the row decompositions

$$e_\mathcal{X}{}' = \begin{pmatrix} s' \\ t \end{pmatrix} \text{ and } e_\mathcal{X}{}'' = \begin{pmatrix} s'' \\ t \end{pmatrix},$$

where $s', s'' \in \mathbb{R}^p$ and $t \in \mathbb{R}^{n_\mathcal{X} - p}$. Due to the above equality, we have that

$$\left(\begin{array}{c|c} \Gamma & \Delta \\ \hline \mathbf{0} & \Lambda \end{array}\right) \cdot \begin{pmatrix} s' \\ t \end{pmatrix} = \mathsf{A} \cdot e_\mathcal{X}{}' = \mathsf{A} \cdot e_\mathcal{X}{}'' = \left(\begin{array}{c|c} \Gamma & \Delta \\ \hline \mathbf{0} & \Lambda \end{array}\right) \cdot \begin{pmatrix} s'' \\ t \end{pmatrix},$$

from which we derive

$$\begin{pmatrix} \Gamma \cdot s' + \Delta \cdot t \\ \Lambda \cdot t \end{pmatrix} = \begin{pmatrix} \Gamma \cdot s'' + \Delta \cdot t \\ \Lambda \cdot t \end{pmatrix}.$$

Therefore, it holds that $\Gamma \cdot s' + \Delta \cdot t = \Gamma \cdot s'' + \Delta \cdot t$ and, so, $\Gamma \cdot s' = \Gamma \cdot s''$, which implies $s' = s''$, being Γ invertible, as already observed in the proof of Claim 2. Consequently, $e_\mathcal{X}{}' = e_\mathcal{X}{}'' \in \mathsf{V}' \cap \mathsf{V}''$. Hence, $e_\mathcal{X} \in \mathsf{A} \cdot (\mathsf{V}' \cap \mathsf{V}'')$. □

Claim 4. $\mathsf{V}_{i+h+1} = \mathsf{A}^i \cdot \mathsf{V}_{h+1} \cap \bigcap_{j=0}^{h+k} \mathsf{A}^j \cdot \mathsf{Z}_{i,j}^\star + z_i^\star$, *for all* $i \in \mathbb{N}$.

Proof. The equality immediately follows by Claim 3 and the (h, k)-periodicity of the transformation matrix A. Indeed, it is enough to intersect together all the polyhedra $\mathsf{Z}^{\star}_{l_1}$ and $\mathsf{Z}^{\star}_{l_2}$, with $l_1 \leq l_2$, associated with power indexes $i - l_1$ and $i - l_2$ such that $h < i - l_2$ and $i - l_1 = i - l_2 + q \cdot h$, for some number $q \in [0, k[$. □

Claim 5. *There are doubly-exponentially (*resp.*, exponentially) many polyhedra (*resp.*, rectangular polyhedra)* $\mathsf{Z}^{\star}_{i,j}$.

Proof. We can finally prove that there are at most doubly-exponentially (*resp.*, exponentially) many reachable (*resp.*, rectangular) polyhedra. Every $\mathsf{Z}^{\star}_{i,j}$ is obtained from the intersection of possibly several polyhedra $\mathsf{Z}^{\star}_{l}$, which are in turn obtained as restriction and translation of the derived condition polyhedra $\mathsf{Y}_1, \ldots, \mathsf{Y}_m$, *w.r.t.* some vector z_i. Due to the boundedness of the invariant I, it is not hard to see that there are at most exponentially many vectors z_i that allow a translation of a polyhedron Y_i to remain inside the invariant. Consequently, in general, every polyhedron $\mathsf{Z}^{\star}_{i,j}$ is the intersection of at most exponentially many polyhedra derived from $\mathsf{Y}_1, \ldots, \mathsf{Y}_m$. Thus, we can have at most doubly-exponentially many polyhedra $\mathsf{Z}^{\star}_{i,j}$. This fact can be also derived by thinking that a convex polyhedron can be uniquely identified by the set of its vertexes and there are at most exponentially many values to be associated with them.

A better estimation can be computed in case the condition polyhedra $\mathsf{Y}_1, \ldots, \mathsf{Y}_m$ are rectangular. Indeed, translations and intersection of rectangular polyhedra are rectangular as well. Consequently, all $\mathsf{Z}^{\star}_{i,j}$ are necessarily rectangular. Now, every such a polyhedron inside the invariant requires only $n_{\mathcal{X}}$ points to be identified, and there are at most exponentially many values that these points can assume. Consequently, in this case the number of possible reachable polyhedra is at most exponential. □