Draft version 150, June 13, 2011.

Model Checking Coverability Graphs of Vector Addition Systems

Michel Blockelet and Sylvain Schmitz

LSV, ENS Cachan & CNRS, Cachan, France
mblockel@dptinfo.ens-cachan.fr, schmitz@lsv.ens-cachan.fr

Abstract

A large number of properties of a vector addition system—for instance coverability, boundedness, or regularity—can be decided using its coverability graph, by looking for some characteristic pattern. We propose to unify the known exponential-space upper bounds on the complexity of such problems on vector addition systems, by seeing them as instances of the model-checking problem for a suitable extension of computation tree logic, which allows to check for the existence of these patterns. This provides new insights into what constitutes a "coverability-like" property.

Keywords. Vector Addition Systems; CTL; Coverability Properties; Complexity.

1 Introduction

Vector addition systems (or equivalently Petri nets) are widely employed to reason about concurrent computations. Many decidable problems for vector addition systems are known to be ExpSpace-hard thanks to a proof originally due to Lipton (Cardoza et al., 1976). Regarding complexity upper bounds, a key distinction arises between "reachability-like" problems on the one hand, for which no upper-bound is currently known in spite of continuous research on the subject (Mayr, 1981; Kosaraju, 1982; Leroux, 2011), and "coverability-like" problems on the other hand, for which ExpSpace upper bounds have been derived after the work of Rackoff (1978). The latter class of problems is known to encompass many questions for the analysis of vector addition systems (prominently linear-time model-checking (Habermehl, 1997)), and related models of concurrency (e.g. Ganty et al., 2009; Kaiser et al., 2010).

We promote in this paper a characterization of "coverability-like" properties as relying on the existence of some witness pattern in the *coverability graph* (Karp and Miller, 1969; Hack, 1974) of the system—this graph provides a finite abstraction of the system's possible behaviours. This stance is backed up by several results (see e.g. Valk and Vidal-Naquet, 1981; Finkel and Sangnier, 2008; Chambart et al., 2011) that rely on the same powerful technique: since the coverability graph is finite, the existence of a witness can be checked, yielding the decidability of the property at hand. As the coverability graph might have non primitive-recursive size (Cardoza et al., 1976), this technique comes however at a very high price—at least at first sight.

We show in this paper that a fragment of *existential computation tree logic* (ECTL) extended with Presburger constraints on paths enjoys a small model property when checked against runs in coverability graphs, and deduce an ExpSpace complexity upper bound for properties expressed in this fragment. These properties encompass many examples of properties testable in exponential space we found in the literature. We further believe the resulting formulæ to be quite natural and intuitive (they can express branching properties and the existence of ω-markings *directly*), and illustrate this point with several examples.

On the technical side, the proof of this small model property is in the line of similar results shown by Rackoff (1978) for the coverability and the boundedness problems, and extended by Yen (1992); Atig and Habermehl (2009); Demri (2010) to more complex properties. These extensions rely on rather terse, ad-hoc logical formalisms, which are checked against the actual runs of the system—it is tempting to blame the complexity of Yen's logical formalism for the issue found in his proof by Atig and Habermehl. Thus a major contribution of the paper is the key insight that what should be checked are runs in coverability graphs instead of actual runs, and that a reasonably standard logic based on CTL is perfectly usable to this end. In more details, we define a notion of VAS coverability graphs that will constitute the models of our logic (Section 2) and investigate their simulation relations; we define an extension of CTL using Presburger constraints on path and atomic propositions testing for coverability (Section 3.1) before considering the decidability of VAS model-checking for some of its fragments (Section 3.2); we then consider a restricted fragment of *eventually increasing* formulæ and prove its VAS model-checking problem to be ExpSpace-complete (Section 4).

Notations. Let $\mathbb{Z}_\omega = \mathbb{Z} \uplus \{\omega\}$ be the set of integers completed with a limit element ω, which is larger than any finite z in $\mathbb{Z}$ and verifies $\omega + d = \omega$ for all d in $\mathbb{Z}$. Whenever working on vectors in $\mathbb{Z}_\omega^k$ for some k, we implicitly employ component-wise orderings. We consider throughout the paper rooted *labeled transition systems* (LTS) $\mathcal{S} = \langle S, \to, \ell, s_{\text{init}}\rangle$ where, for some $k \geq 1$, S is a set of states, ℓ is a state labeling function from S to $\mathbb{Z}_\omega^k$, s_{init} is the initial state in S, and $\to$ is a labeled transition relation included in $S \times \mathbb{Z}^k \times S$. In our developments we ignore labels and define the *size* $|\mathcal{S}|$ of a LTS $\mathcal{S}$ as the cardinality of $\to$, and for a set of vectors $\mathsf{V} \subseteq \mathbb{Z}_\omega^k$, $\|\mathsf{V}\| = \max_{\mathsf{v}\in\mathsf{V},1\leq j\leq k,\mathsf{v}(j)<\omega}(0, \lceil\log_2(|\mathsf{v}(j)|) + 1\rceil)$. An LTS is called *tree-shaped* if any state has at most one predecessor by $\to$, i.e. for all s, $|\{s' \in S \mid s' \to s\}| \leq 1$, and *path-shaped* if furthermore it has at most one successor by $\to$, i.e. for all s, $|\{s' \in S \mid s \to s'\}| \leq 1$.

2 Coverability Graphs

Let us first recall the definition of coverability graphs for vector addition systems and how they can be used to decide various properties.

Vector Addition Systems. A *k-dimensional vector addition system* (k-VAS) is a pair $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0\rangle$ where V is a finite set of transitions in $\mathbb{Z}^k$ and x_0 an initial marking in $\mathbb{N}^k$ (Karp and Miller, 1969). Formally, we can define the *reachability* *graph* of such a k-VAS as the (generally infinite) LTS $R(\mathcal{S}) = \langle \mathbb{N}^k, \rightarrow, id, \mathsf{x}_0 \rangle$ with states (also called *markings*) in $\mathbb{N}^k$, the identity id as state labeling function, and transitions labels in V s.t. $\mathsf{x} \xrightarrow{\mathsf{a}} \mathsf{x}'$ iff $\mathsf{x}+\mathsf{a} = \mathsf{x}'$ (note that it implies $\mathsf{x}+\mathsf{a} \geq \mathsf{0}$). In some proofs, we will consider *generalized VAS*, where x_0 can be taken from $\mathbb{Z}^k_\omega$. We consider several parameters for VAS size, as do Rosier and Yen (1986): the size of the binary encoding of the largest difference a vector from the transitions set can induce $\|\mathsf{V}\|$, the cardinal of the transition relation $|\mathsf{V}|$, and the dimension k.

Canonical Coverability Graph. Coverability graphs are finite abstractions of VAS reachability graphs. In order to remain finite, they employ markings over the complete space $(\mathbb{N} \uplus \{\omega\})^k$, noted $\mathbb{N}^k_\omega$. There are several possible definitions for coverability graphs, all based on the original Karp and Miller coverability tree construction (Karp and Miller, 1969); here is a particular flavour, as found for instance in (Valk and Vidal-Naquet, 1981)

Given a LTS $\langle S, \rightarrow, \ell, s_{\text{init}} \rangle$ and given some $1 \leq j \leq k$, let us first define a *j-antecedent* of a pair (s, a) in $S \times \mathbb{Z}^k$ as a state s' satisfying

$$s_{\text{init}} \rightarrow^* s' \xrightarrow{w} s \wedge \ell(s') \leq \ell(s) + \mathsf{a} \wedge \ell(s')(j) < (\ell(s) + \mathsf{a})(j) \tag{1}$$

for some w in $(\mathbb{Z}^k)^*$. A j-antecedent witnesses the fact that, by repeating the sequence of transitions $w\mathsf{a}$ from s', we can obtain arbitrarily high values in coordinate j—which will be represented symbolically by an ω value in the coverability graph.

The *coverability tree* of a k-VAS $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ is a tree-shaped LTS $T(\mathcal{S}) = \langle S, \rightarrow, \ell, s_{\text{init}} \rangle$ with state labels in $\mathbb{N}^k_\omega$ and transition labels in V constructed by:

basis initially $S = \{s_{\text{init}}\}$ with label $\ell(s_{\text{init}}) = \mathsf{x}_0$ and s_{init} is flagged as unprocessed,

step for every unprocessed state s and every a in V

- if $\ell(s) + \mathsf{a} \not\geq \mathsf{0}$: do nothing, as a is not firable in $\ell(s)$,
- otherwise, let s' be a fresh state, update S to be $S \uplus \{s'\}$, add a transition $s \xrightarrow{\mathsf{a}} s'$, and set the label of s' in $\mathbb{N}^k_\omega$ to

$$\ell(s')(j) \stackrel{\text{def}}{=} \begin{cases} \omega & \text{if } \exists s'' \text{ a } j\text{-antecedent of } (s, \mathsf{a}) \\ (\ell(s) + \mathsf{a})(j) & \text{otherwise} \end{cases} \tag{2}$$

If there does not exist any state s'' in S with $\ell(s') = \ell(s'')$ and $s_{\text{init}} \rightarrow^* s'' \rightarrow^* s$, flag s' as unprocessed; s' is otherwise a leaf of the tree.

The *canonical coverability graph* $C(\mathcal{S})$ of a k-VAS $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ is obtained by identifying identically-labeled states in $T(\mathcal{S})$, i.e. it is the quotient $C(\mathcal{S}) = T(\mathcal{S})/{\equiv}$ for the equivalence relation $s \equiv s'$ iff $\ell(s) = \ell(s')$ (see e.g. Figure 1).

Examples of Coverability Properties. Coverability graphs allow to decide many properties on a k-VAS $\mathcal{S}$; for instance,

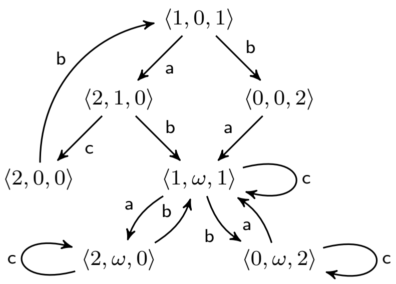

Figure 1: The canonical coverability graph for the VAS $\mathcal{S} = \langle\{\mathsf{a}, \mathsf{b}, \mathsf{c}\}, \langle 1, 0, 1\rangle\rangle$ with transitions $\mathsf{a} = \langle 1, 1, -1\rangle$, $\mathsf{b} = \langle -1, 0, 1\rangle$, and $\mathsf{c} = \langle 0, -1, 0\rangle$.

coverability given a marking x in $\mathbb{N}^k$, whether a marking $\mathsf{x}' \geq \mathsf{x}$ is reachable in $R(\mathcal{S})$—simply check whether a state s with $\ell(s) \geq \mathsf{x}$ is reachable in $C(\mathcal{S})$; for instance in Figure 1 we see that $\langle 1, 5, 1\rangle$ is coverable but $\langle 2, 1, 2\rangle$ is not—,

boundedness whether the set of reachable markings in $R(\mathcal{S})$ is finite—this occurs iff no ω value appears in the label of any state of $C(\mathcal{S})$; for instance in Figure 1 the VAS is not bounded—,

place boundedness given a coordinate $1 \leq j \leq k$, whether the set of values $\mathsf{x}(j)$ for all reachable x in $R(\mathcal{S})$ is finite—this occurs iff no ω value appears as $\ell(s)(j)$ for some state s of $C(\mathcal{S})$; for instance in Figure 1, the second coordinate is unbounded but the other two are bounded,

language regularity whether the *language*, i.e. the set of labels w in V^* of transition sequences $s_0 \xrightarrow{w} s$ in $R(\mathcal{S})$, is regular—this occurs if no state s with a cycle $s \xrightarrow{\mathsf{a}_1\cdots\mathsf{a}_n} s$ appears in $C(\mathcal{S})$ s.t. there exists $1 \leq j \leq k$, $\ell(s)(j) = \omega$ and $\left(\sum_{i=1}^{n} \mathsf{a}_i\right)(j) < 0$ (Valk and Vidal-Naquet, 1981, Theorem 5); for instance in Figure 1 we find one such cycle $\langle 1, \omega, 1\rangle \xrightarrow{\mathsf{c}} \langle 1, \omega, 1\rangle$, and indeed the language of this VAS yields $(\mathsf{ab})^n\mathsf{c}^{\leq n}$ when intersected with $(\mathsf{ab})^*\mathsf{c}^*$, and is therefore non-regular.

All these properties are decidable in exponential space; see (Rackoff, 1978) for the first two, and (Demri, 2010) for the last two. Observe that we were able to characterize each property by the existence of some witness in the canonical coverability graph; we shall see in Section 3 that we can easily express those properties in a modal logic, and later in Section 4 that the exponential space upper bound applies to all properties expressed in this logic.

Partial Covers. In preparation of the technical developments of the following sections, we define structures related to the coverability graph that will serve as witnesses. The motivation is that later we will build small models for properties by induction on the dimension, thus it will be convenient to consider *partial* coverability graphs, which are "correct" only on the first j coordinates out of k.

Definition 2.1. A *partial cover* for a generalized k-VAS $\langle \mathsf{V}, \mathsf{x}_0\rangle$ is an accessible LTS $\langle S, \rightarrow, \ell, s_{\text{init}}\rangle$ with transition labels in V s.t. $\ell(s_{\text{init}}) = \mathsf{x}_0$ and, if $s \xrightarrow{\mathsf{a}} s'$, then for all $1 \leq j \leq k$, either $\ell(s)(j) + \mathsf{a}(j) = \ell(s')(j)$, or $\ell(s)(j) < \omega$, $\ell(s')(j) = \omega$, and on every path $s_{\text{init}} = s_0 \xrightarrow{\mathsf{a}_1} \cdots \xrightarrow{\mathsf{a}_n} s_n = s$, there exists $0 \leq i \leq n$ s.t. s_i is a j-antecedent of (s, a) (see (1)).

Thus a partial cover does not enforce positive values on the state labels, but guarantees transition labels to be compatible with state labels, and ω values to be introduced only when legal, i.e. when at least one j-antecedent exists on every path from the initial state. Partial covers can also be seen as LTS with j-antecedency relations—in addition to the transition relation—from a state with a newly introduced ω value to each of its j-antecedents. When constructing partial covers we will need to preserve the existence of at least one such j-antecedent.

With the example of Figure 1, the system reduced to the initial marking

$$\langle 1, 0, 1\rangle \tag{3}$$

is a partial cover, the following are two more (path-shaped) partial covers of the same VAS:

$$\langle 1, 0, 1\rangle \xrightarrow{\mathsf{a}} \langle 2, 1, 0\rangle \xrightarrow{\mathsf{a}} \langle 3, 2, -1\rangle \tag{4}$$

$$\langle 1, 0, 1\rangle \xrightarrow{\mathsf{a}} \langle 2, 1, 0\rangle \xrightarrow{\mathsf{b}} \langle 1, \omega, 1\rangle \xrightarrow{\mathsf{c}} \langle 1, \omega, 1\rangle \ , \tag{5}$$

and this last one is not a partial cover, as we cannot introduce an ω value at this point:

$$\langle 1, 0, 1\rangle \xrightarrow{\mathsf{a}} \langle 2, \omega, 0\rangle \ . \tag{6}$$

Definition 2.2. Let $0 \leq i \leq k$. A partial cover $\mathcal{C} = \langle S, \rightarrow, \ell, s_{\text{init}}\rangle$ is *i-admissible* if for all $1 \leq j \leq i$ and for all s in S, $0 \leq \ell(s)(j)$.

Note that in particular the initial marking x_0 of a generalized k-VAS also needs to satisfy $\mathsf{x}_0(j) \geq 0$ for $1 \leq j \leq i$ in order for a i-admissible partial cover to even exist. Both the canonical coverability graph and the reachability graph of a k-VAS are k-admissible partial covers. Among the previous examples, (3) and (5) are 3-admissible, (4) is 2-admissible but not 3-admissible. Considering our examples of coverability properties, the LTS in (5) could be used as a witness of coverability of $\langle 1, 5, 1\rangle$, unboundedness in the second coordinate, and non regularity of the language.

Covering Simulations. Among all the k-admissible partial covers of a k-VAS $\mathcal{S}$ (Defs. 2.1 and 2.2), we find in particular its canonical coverability graph $C(\mathcal{S})$. All these k-admissible partial covers are in fact related to $C(\mathcal{S})$ by a *simulation* relation (see App. A.1 for details):

Definition 2.3. Let $k \geq 1$ and $\mathcal{S}_1 = \langle S_1, \rightarrow_1, \ell_1, s_1\rangle$ and $\mathcal{S}_2 = \langle S_2, \rightarrow_2, \ell_2, s_2\rangle$ be two LTS. A *covering simulation* between $\mathcal{S}_1$ and $\mathcal{S}_2$ is a relation $R \subseteq S_1 \times S_2$ s.t.

1. $s_1 \ R \ s_2$,
2. if $s \ R \ s'$, then
   (a) $\ell_1(s) \leq \ell_2(s')$ and
   (b) if $s \xrightarrow{\mathsf{a}}_1 q$ for some a in $\mathbb{Z}^k$ and q in S_1 then there exists q' in S_2 with $s' \xrightarrow{\mathsf{a}}_2 q'$ and $q \ R \ q'$.

We say that $\mathcal{S}_2$ *simulates* $\mathcal{S}_1$, noted $\mathcal{S}_1 \preccurlyeq \mathcal{S}_2$, if there exists a covering simulation R between $\mathcal{S}_1$ and $\mathcal{S}_2$.

Lemma 2.4. *Let $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a k-VAS and $\mathcal{C}$ a k-admissible partial cover of $\mathcal{S}$. Then $\mathcal{C} \preccurlyeq C(\mathcal{S})$.*

3 CTL Logics for Coverability Graphs

We first propose a very general logic based on CTL for model-checking coverability graphs (Section 3.1). Our purpose with this general logic is to motivate our choice of CTL fragment for the following sections: indeed, the full logic will turn out to be too powerful, and we will restrict ourselves to an existential fragment with a decidable model checking problem (Section 3.2).

3.1 An Extension of CTL

We define an extension $\mathrm{PrCTL}_{\geq}(\mathsf{U})$ of CTL specifically designed to express properties of VAS coverability graphs. It features

coverability constraints $\mu(j) \geq c$, where c is a constant in $\mathbb{N}_\omega$, as atomic formulæ, allowing to express that the label in the current state has value greater or equal to c in its jth coordinate. These extend the usual coverability constraints (see e.g. Esparza, 1997) by also allowing to express $\mu(j) = \omega$.

Presburger-refined temporal modalities U_ψ using Presburger formulæ ψ to constrain the allowed paths—this is similar to the regular modalities found for instance in (Axelsson et al., 2010), but what is constrained here is the *effect* of a transition sequence rather than its label.

Presburger Formulæ. We restrict our attention to quantifier-free Presburger (QFP) formulæ, since one such formula can be obtained from any Presburger formula at the expense of a worst-case triple exponential blowup (see e.g. Weispfenning, 1990, Theorem 2.1). More precisely, given an infinite countable set of variables $\mathcal{X}$, a QFP formula ψ is defined through

$$\psi ::= \top \mid \neg\psi \mid \psi \vee \psi \mid \alpha, \quad \alpha ::= \tau \geq \tau \mid \tau \equiv_p \tau, \quad \tau ::= 0 \mid 1 \mid x \mid \tau + \tau \tag{7}$$

where x is a variable from $\mathcal{X}$ and $p \geq 2$.[1] Given a vector x of values in $\mathbb{Z}^k$ and a formula ψ with k free variables $x_1, \ldots, x_k$, we write $\psi(\mathsf{x})$ for the closed formula with $\mathsf{x}(j)$ substituted for x_j for each $1 \leq j \leq k$. Given a closed Presburger formula ψ, we write $\mathrm{PA} \models \psi$ if the formula is valid.

Syntax of $\mathbf{PrCTL}_{\geq}(\mathsf{U})$. Formally, fix some k in $\mathbb{N}$; a k-formula of $\mathrm{PrCTL}_{\geq}(\mathsf{U})$ is a term φ defined by the abstract syntax

$$\varphi ::= \top \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathsf{E}(\varphi \, \mathsf{U}_\psi \, \varphi) \mid \mu(j) \geq c$$

[1] We include the *divisibility* relations, which are required for quantifier elimination, with semantics $x \equiv_p y$ iff $\exists z. x + pz = y$ for all x, y in $\mathbb{Z}$ and $p \geq 2$.

where ψ denotes a QFP formula with k free variables, $1 \leq j \leq k$, and c is a constant in $\mathbb{N}_\omega$. Note that a k-formula is also a k'-formula for all $k' \geq k$. We can simulate the classical "next" modalities X (see the proof of Proposition 3.1). The classical, unrefined U modality can be defined by $\mathsf{E}(\varphi \mathrel{\mathsf{U}} \varphi') \stackrel{\text{def}}{=} \mathsf{E}(\varphi \mathrel{\mathsf{U}_\top} \varphi')$ using the $\top$ formula of QFP. We also define as usual $\mathsf{EF}_\psi \varphi \stackrel{\text{def}}{=} \mathsf{E}(\top \mathrel{\mathsf{U}_\psi} \varphi)$, and the dualities $\bot \stackrel{\text{def}}{=} \neg\top$, $\varphi \wedge \varphi' \stackrel{\text{def}}{=} \neg((\neg\varphi) \vee (\neg\varphi'))$, $(\mu(j) < c) \stackrel{\text{def}}{=} \neg(\mu(j) \geq c)$, and $\mathsf{AG}_\psi \varphi \stackrel{\text{def}}{=} \neg\mathsf{EF}_\psi \neg\varphi$.

Semantics of PrCTL$_\geq$(U). The models of PrCTL$_\geq$(U) formulæ are labeled transition systems $\langle S, \rightarrow, \ell, s_{\text{init}} \rangle$. Given a state s in S, write *Paths*(s) for the set of *maximal paths* $\pi = s_0 \xrightarrow{\mathsf{a}_1} s_1 \xrightarrow{\mathsf{a}_2} \cdots$ starting in $s = s_0$ and where each a_i is in $\mathbb{Z}^k$ and each s_i in S. The path is either infinite with length $|\pi| = \omega$, or finite of form $\pi = s_0 \xrightarrow{\mathsf{a}_1} \cdots \xrightarrow{\mathsf{a}_n} s_n$ if s_n has no successor and then $|\pi| = n$. If $\mathsf{a}_1 \cdots \mathsf{a}_n$ is a sequence in $(\mathbb{Z}^k)^*$ (with $n = 0$ for the empty sequence), then its *effect* is $\Delta \mathsf{a}_1 \cdots \mathsf{a}_n = \sum_{i=1}^n \mathsf{a}_i$ in $\mathbb{Z}^k$.

A state s in S *satisfies* a PrCTL$_\geq$(U) formula φ, written $s \models \varphi$, in the following inductive cases:

$$\begin{array}{ll}
s \models \top & \text{always,} \\
s \models \neg\varphi & \text{iff } s \not\models \varphi\ , \\
s \models \varphi_1 \vee \varphi_2 & \text{iff } s \models \varphi_1 \text{ or } s \models \varphi_2\ , \\
s \models \mathsf{E}(\varphi \mathrel{\mathsf{U}_\psi} \varphi') & \text{iff } \exists \pi = s_0 \xrightarrow{\mathsf{a}_1} s_1 \xrightarrow{\mathsf{a}_2} \cdots \in \mathit{Paths}(s),\ \exists n \leq |\pi|, \\
 & \quad \text{PA} \models \psi(\Delta \mathsf{a}_1 \cdots \mathsf{a}_n),\ s_n \models \varphi', \text{ and } \forall m < n,\ s_m \models \varphi, \\
s \models \mu(j) \geq c & \text{iff } \ell(s)(j) \geq c\ .
\end{array}$$

As usual, a LTS $\mathcal{S}$ satisfies φ, written $\mathcal{S} \models \varphi$, if $s_{\text{init}} \models \varphi$. A k-VAS $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ *satisfies* a PrCTL$_\geq$(U) k-formula φ, written $\langle \mathsf{V}, \mathsf{x}_0 \rangle \models \varphi$, if there exists a k-admissible partial cover $\mathcal{C}$ of $\langle V, \mathsf{x}_0 \rangle$ such that $\mathcal{C} \models \varphi$. We will see later (Proposition 3.2) that for *existential* PrCTL$_\geq$(U) this boils down to model-checking the canonical coverability graph.

Examples of Formulæ. Consider once more the coverability properties of Section 2: the coverability problem for a marking x can be checked by model-checking these formulæ against $\mathcal{C}(\mathcal{S})$:

$$\varphi_{\text{cov},\mathsf{x}} \stackrel{\text{def}}{=} \mathsf{EF} \bigwedge_{j=1}^{k} \mu(j) \geq \mathsf{x}(j)\ ; \tag{8}$$

unboundedness by

$$\varphi_{\text{unb}} \stackrel{\text{def}}{=} \mathsf{EF} \bigvee_{j=1}^{k} \mu(j) \geq \omega\ ; \tag{9}$$

place unboundedness in coordinate $1 \leq j \leq k$ by

$$\varphi_{\text{unb},j} \stackrel{\text{def}}{=} \mathsf{EF} \mu(j) \geq \omega\ ; \tag{10}$$

non-regularity of the language by

$$\varphi_{\text{unreg}} \overset{\text{def}}{=} \mathsf{EF} \bigvee_{\substack{I \subseteq \{1,\ldots,k\} \\ I \neq \emptyset}} \quad \bigvee_{I \subseteq J \subseteq \{1,\ldots,k\}} \left(\bigwedge_{j \in J} \mu(j) \geq \omega \wedge \mathsf{EF}_{\psi_{I,J}} \top \right) \tag{11}$$

where

$$\psi_{I,J}(x_1,\ldots,x_k) \overset{\text{def}}{=} \bigwedge_{j \in I} x_j < 0 \wedge \bigwedge_{j \notin J} x_j \geq 0\;. \tag{12}$$

We can check that the 3-admissible partial cover (5) satisfies all these formulæ (setting $\mathsf{x} = \langle 1,5,1 \rangle$ for (8)), thus our example VAS satisfies all these formulæ.

3.2 VAS Model Checking

We turn now to the *VAS model checking problem*: for a VAS $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ and a PrCTL$_\geq$ formula φ, does $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ satisfy φ?

Undecidability of PrCTL$_\geq(\mathsf{U})$. When considering how general PrCTL$_\geq$ is, its model-checking problem is rather unsurprisingly undecidable, even if restricted to EF modalities, i.e. for the PrCTL$_\geq(\mathsf{F})$ fragment (the proof uses results by Esparza (1997); see App. A.2):

Proposition 3.1. *The VAS model-checking problem for PrCTL$_\geq(\mathsf{F})$ is undecidable.*

Decidability of PrECTL$_\geq(\mathsf{U})$. The formulæ used in the proof of Proposition 3.1 employ alternation in a crucial way in order to encode the VAS containment problem, and a natural question is whether the *existential* fragment PrECTL$_\geq(\mathsf{U})$, with syntax

$$\varphi ::= \top \mid \bot \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathsf{E}(\varphi \; \mathsf{U}_\psi \; \varphi) \mid \mu(j) \geq c\;,$$

is decidable. This is the case: it suffices to check whether the canonical coverability graph satisfies the formula, since by Lemma 2.4 it *simulates* any other k-admissible partial cover. This is one of the benefits of considering CTL fragments rather than ad-hoc logics: the standard toolkit of modal logic is readily applicable, like the connection between simulations and existential CTL (see App. A.3 for details):

Proposition 3.2. *The VAS model-checking problem for PrECTL$_\geq(\mathsf{U})$ is decidable in nondeterministic polynomial time in $|C(\mathcal{S})|$ and $|\varphi|$.*

The decidability of VAS model-checking for PrECTL$_\geq(\mathsf{U})$ is encouraging, but our decision procedure relies on the construction of the canonical coverability graph $C(\mathcal{S})$. As the latter can have non primitive-recursive size (Cardoza et al., 1976, who attribute the idea to Hack), this is not a very efficient algorithm: it yields an Ackermannian upper bound (Figueira et al., 2011, Section VII.C) on the complexity of VAS model-checking for PrECTL$_\geq(\mathsf{U})$. This is a ridiculously high upper bound, but we actually suspect the VAS model-checking problem for PrECTL$_\geq(\mathsf{U})$ to be Ackermann-complete. On the one hand, Proposition 3.2 implies the PrECTL$_\geq(\mathsf{U})$ problem to be in NPTime for fixed VAS; on the other hand, small extensions within existential fragments quickly lead to undecidability (e.g. when allowing $\mu(j) < c$ or G_ψ; see App. B.1 for a discussion).

The remainder of the paper is dedicated to a fragment of PrECTL$_\geq(\mathsf{F})$ for which we demonstrate a small model property and deduce decision procedures working in exponential space. Although we use techniques adapted from Rackoff and his successors, several points make these contributions stand out: the *simplicity* of the logic, its ability to express *branching* properties directly, and its intuitive semantics in terms of *coverability graphs*.

4 Eventually Increasing Formulæ

Let us consider the PrECTL$_\geq(\mathsf{F})$ fragment. We are going to introduce a semantic restriction to PrECTL$_\geq(\mathsf{F})$ formulæ, inspired by a similar restriction employed by Atig and Habermehl (2009) to fix Yen (1992)'s proof.

4.1 The PrECTL$_\geq(\mathsf{F})$ Fragment

Eventually Increasing Formulæ. We can restrict ourselves to finite tree-shaped models for PrECTL$_\geq(\mathsf{F})$ formulæ; such a model $\mathcal{C}$ has a root s and a number of leaves $s_1, \ldots, s_n$, each satisfying some *coverability constraint* (CC) subformula γ, of form

$$\gamma ::= \top \mid \bot \mid \gamma \wedge \gamma \mid \gamma \vee \gamma \mid \mu(j) \geq c\,, \tag{13}$$

where $1 \leq j \leq k$ and c is in $\mathbb{N}_\omega$. We call this model *increasing* if $\ell(s_i) \geq \ell(s)$ for all $1 \leq i \leq n$. A formula φ of PrECTL$_\geq(\mathsf{F})$ is *increasing* if all its tree-shaped models are increasing. An *eventually increasing formula* is a formula of form $\mathsf{EF}\varphi$ for some increasing formula φ. We denote the set of (eventually) increasing PrECTL$_\geq(\mathsf{F})$ formulæ by (e)iPrECTL$_\geq(\mathsf{F})$. All our example formulæ (8)–(11) are eventually increasing.

Such a semantic restriction naturally leads to the question: is it decidable whether a formula fits into the fragment? We first consider the related problem of PrECTL$_\geq(\mathsf{F})$ satisfiability: given a k-formula φ, does there exist a k-VAS $\langle\mathsf{V}, \mathsf{x}_0\rangle$ s.t. $\langle\mathsf{V}, \mathsf{x}_0\rangle \models \varphi$? It turns out that this satisfiability problem reduces to the satisfiability of its QFP subformulæ, which can be checked in NPTime (see App. A.4):

Proposition 4.1. *The satisfiability problem for PrECTL$_\geq(\mathsf{F})$ is decidable in* NPTime.

Checking whether a formula is increasing is a bit more involved: we need to check whether the various QFP subformulæ ensure every possible model is increasing, which we do by constructing a (universal) Presburger formula (see App. A.5):

Proposition 4.2. *Let φ be a k-formula of PrECTL$_\geq(\mathsf{F})$. Whether φ is a k-formula of iPrECTL$_\geq(\mathsf{F})$ is decidable in* NPTime.

4.2 Small Model Properties

The proof of the small model property for eiPrECTL$_\geq(\mathsf{F})$ formulæ follows the general design of Rackoff's proof: first a small model property on models with *bounded* values (Lemma 4.3) using results on the existence of small solutions for linear integer programming, and then a proof of existence of a small model in general by induction on the dimension (Lemma 4.4).

Bounded Models. Define as usual with Rackoff's approach an (i, r)-*bounded* LTS as an i-admissible one where no finite value on the first i coordinates is larger than r: for all s and every $1 \leq j \leq i$, $\ell(s)(j) \geq r$ implies $\ell(s)(j) = \omega$. If $i \leq k$, the i-*projection* of a formula φ is a formula $\varphi_{|_i}$ where every $\mu(j) \geq c$ term of φ with $j > i$ and $c < \omega$ has been replaced by $\top$. Adapting the proof of (Rackoff, 1978, Lemma 4.5) to our case, we obtain (see App. A.6 for details):

Lemma 4.3 (Small Models for Bounded LTS)**.** *Let $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a generalized k-VAS with $k > 1$, φ be a PrECTL$_{\geq}(\mathsf{F})$ formula, and $0 \leq i \leq k$ and $r \geq 0$. If there exists an (i, r)-bounded partial cover $\mathcal{C}$ of $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ s.t. $\mathcal{C} \models \varphi_{|_i}$, then there exists a tree-shaped (i, r)-bounded partial cover $\mathcal{C}'$ of $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ with $\mathcal{C}' \models \varphi_{|_i}$ and $|\mathcal{C}'| \leq (2^{\|\mathsf{V}\|} r)^{(k+|\varphi|)^d}$ for some constant d (independent of V, x_0, k, φ, i, and r).*

General Models. We prove now a general small model property for eiPrECTL$_{\geq}(\mathsf{F})$ formulæ. It borrows several elements from earlier research, prominently (Rackoff, 1978, Lemma 4.6 & 4.7), but also crucially the use of an increasing condition to allow "replaying" a model at a leaf (Atig and Habermehl, 2009). Given $\mathsf{V} \subseteq (\mathbb{Z}_\omega)^k$, a k-coverability formula φ, and some $0 \leq i < k$, let

$$g(0) \stackrel{\text{def}}{=} (2^{\|\mathsf{V}\|} \cdot |\mathsf{V}|)^{(k+|\varphi|)^d}$$

$$g(i+1) \stackrel{\text{def}}{=} \Big(2^{\|\mathsf{V}\|} \cdot (2^{\|\mathsf{V}\|} g(i) + |\varphi|)\Big)^{(k+|\varphi|)^d} + 1 + g(i)$$

where d is the constant of Lemma 4.3. We finally obtain our small model property (see App. A.7 for a proof):

Lemma 4.4 (Small Model Property)**.** *Let $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a generalized k-VAS and $\varphi = \mathsf{EF}\varphi'$ be a k-eventually increasing formula. Let $\varphi_{|_i}$ be satisfiable. Then there exists a tree-shaped i-admissible partial cover of $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ that models $\varphi_{|_i}$ and of size $\leq g(i)$.*

Lemma 4.4 results in a doubly exponential bound on the size of a k-admissible model for an eventually increasing formula, from which an ExpSpace algorithm can be designed, which is optimal considering the ExpSpace lower bound (Cardoza et al., 1976):

Theorem 4.5 (Complexity of VAS model checking)**.** *The VAS model-checking problem for eiPrECTL$_{\geq}(\mathsf{F})$ formulæ is* ExpSpace*-complete.*

See App. A.8 for details. Note that the different parameters on the size of the VAS and of the formula influence this complexity differently: for fixed k the obtained algorithm works in PSpace. A matching PSpace lower bound on the place coverability problem is given by Rosier and Yen (1986, Corollary 3.1) for fixed $k \geq 4$.

Another interesting consequence of our bounds is that bounds for model checking vector addition systems *with states* (VASS) are easy to derive; for instance by encoding a k-VASS with state-space Q into a $(k + 2\lceil \log_2 |Q| \rceil)$-VAS:

this is not as tight as the $(k+3)$-VAS encoding of Hopcroft and Pansiot (1979), but allows to test in which control state we are in an eiPrECTL$_{\geq}(\mathsf{F})$ formula using coverability constraints $\mu(j) \geq 1$. Thus the number $|Q|$ of states only influences polynomially the complexity of VASS model checking for eiPrECTL$_{\geq}(\mathsf{F})$.

4.3 Related Work

The first attempt at unifying ExpSpace upper bounds on VAS problems was proposed by Yen (1992). This provided ExpSpace upper bounds for many problems (boundedness, coverability, self-coverability, etc.; see Section 4 in (Yen, 1992)). For instance, we can consider the place boundedness problem: a path formula for it has to guess nondeterministically a sequence π of introductions of ω-values leading to the desired unboundedness of place j. Let Π be the set of repetition-free sequences π over $\{1,\ldots,k\}\backslash\{j\}$ and $|\Pi| = n$; write $c(\pi)$ for the set of elements appearing in π and $\pi[i..k]$ for the factor of π between indices i and k (inclusive):

$$\begin{aligned} &\exists\mu_1,\ldots,\mu_{2n+2}, \exists\sigma_1,\ldots,\sigma_{2n+2}(\mu_0 \xrightarrow{\sigma_1} \mu_1 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_{2n+2}} \mu_{2n+2}) \\ \wedge \bigvee_{\pi\in\Pi} &\left(\mu_{2n+1}(j) < \mu_{2n+2}(j) \wedge \bigwedge_{i\notin c(\pi)} \mu_{2n+1}(i) \leq \mu_{2n+2}(i)\right) \\ &\wedge \bigwedge_{m=1}^{|\pi|} \left(\mu_{2m-1}(\pi[m..m]) < \mu_{2m}(\pi[m..m]) \wedge \bigwedge_{i\notin c(\pi[1..m])} \mu_{2m-1}(i) < \mu_{2m}(i)\right). \end{aligned}$$

The first main conjunct under the scope of the choice of π checks that an ω-value can appear in place j. The second main conjunct verifies the same for each element of π in sequence.

The proof of (Yen, 1992) was flawed, and corrected by Atig and Habermehl (2009) who introduced the *increasing* restriction to Yen's logic to characterize formulæ for which the ExpSpace bound held. Nevertheless, this restriction meant that some of the bounds claimed by Yen did not hold any longer, for instance for the regularity problem, and the above formula for place unboundedness is another instance of a non-increasing formula. Demri (2010) finally proposed to relax the class of models by considering "pseudo-runs" instead of actual runs, and provided a formal framework (*general unboundedness properties*) to express properties on such runs, allowing him to prove ExpSpace upper bounds for several open problems like place boundedness, regularity, strong promptness, etc. This is the most closely related approach.

We can express general unboundedness properties as PrECTL$_{\geq}(\mathsf{F})$ formulæ, but not as eventually increasing ones, because these properties only enforce local increasing conditions instead of the global one we employed in this work. On the other hand many aspects of eiPrECTL$_{\geq}(\mathsf{F})$ formulæ are beyond the reach of general unboundedness properties, since for instance we allow full Presburger arithmetic, and can nest EF_{ψ} modalities directly (general unboundedness properties would intersperse plain EF modalities between any two Presburger-refined modalities). This opens the question whether we could design a larger fragment of PrECTL$_{\geq}(\mathsf{F})$ with an ExpSpace-easy VAS model-checking problem and capturing general unboundedness properties.

We believe eiPrECTL$_\geq(\mathsf{F})$ formulæ to be much easier to write than general unboundedness properties; for instance for place unboundedness, one would also have to write explicitly all the different permutations on the order in which ω-values can be introduced in a general unboundedness property, instead of the straightforward formula (10).

References

Atig, M.F. and Habermehl, P., 2009. On Yen's path logic for Petri nets. In Bournez, O. and Potapov, I., editors, *RP 2009*, *3rd Workshop on Reachability Problems*, volume 5797 of *Lecture Notes in Computer Science*, pages 51–63. Springer. doi:10.1007/978-3-642-04420-5_7.

Axelsson, R., Hague, M., Kreutzer, S., Lange, M., and Latte, M., 2010. Extended computation tree logic. In Fermüller, C.G. and Voronkov, A., editors, *LPAR 2010*, *17th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning*, volume 6397 of *Lecture Notes in Computer Science*, pages 67–81. Springer. doi:10.1007/978-3-642-16242-8_6.

Cardoza, E., Lipton, R.J., and Meyer, A.R., 1976. Exponential space complete problems for Petri nets and commutative semigroups. In *STOC'76*, *Eigth Symposium on Theory of Computing*, pages 50–54. ACM Press. doi:10.1145/800113.803630.

Chambart, P., Finkel, A., and Schmitz, S., 2011. Forward analysis and model-checking for trace-bounded WSTS. In Kristensen, L.M. and Petrucci, L., editors, *Petri Nets 2011*, *32nd International Conference on Application and Theory of Petri Nets*, Lecture Notes in Computer Science. Springer.

Demri, S., 2010. On selective unboundedness of VASS. In Chen, Y.F. and Rezine, A., editors, *INFINITY 2010*, *12th International Workshop on Verification of Infinite-State Systems*, volume 39 of *Electronic Proceedings in Theoretical Computer Science*, pages 1–15. doi:10.4204/EPTCS.39.1.

Esparza, J., 1997. Decidability of model checking for infinite-state concurrent systems. *Acta Informatica*, 34(2):85–107. doi:10.1007/s002360050074.

Figueira, D., Figueira, S., Schmitz, S., and Schnoebelen, Ph., 2011. Ackermannian and primitive-recursive bounds with Dickson's Lemma. In *LICS 2011*, *26th Annual IEEE Symposium on Logic in Computer Science*. IEEE. arXiv:1007.2989.

Finkel, A. and Sangnier, A., 2008. Reversal-bounded counter machines revisited. In Ochmański, E. and Tyszkiewicz, J., editors, *MFCS 2008*, *33rd International Symposium on Mathematical Foundations of Computer Science*, volume 5162 of *Lecture Notes in Computer Science*, pages 323–334. Springer. doi:10.1007/978-3-540-85238-4_26.

Ganty, P., Majumdar, R., and Rybalchenko, A., 2009. Verifying liveness for asynchronous programs. In *POPL 2009*, *36th Annual Symposium on Principles of Programming Languages*, pages 102–113. ACM Press. doi:10.1145/1594834.1480895.

Habermehl, P., 1997. On the complexity of the linear-time μ-calculus for Petri nets. In Azéma, P. and Balbo, G., editors, *ICATPN'97*, *18th International Conference on Application and Theory of Petri Nets*, volume 1248 of *Lecture Notes in Computer Science*, pages 102–116. Springer. doi: 10.1007/3-540-63139-9_32.

Hack, M., 1974. Decision problems for Petri nets and vector addition systems. Computation structures group memo 95, Project MAC, MIT.

Hopcroft, J. and Pansiot, J.J., 1979. On the reachability problem for 5-dimensional vector addition systems. *Theoretical Computer Science*, 8(2): 135–159. doi:10.1016/0304-3975(79)90041-0.

Kaiser, A., Kroening, D., and Wahl, T., 2010. Dynamic cutoff detection in parameterized concurrent programs. In Touili, T., Cook, B., and Jackson, P., editors, *CAV 2010*, *22nd International Conference on Computer Aided Verification*, volume 6174 of *Lecture Notes in Computer Science*, pages 645–659. Springer. doi:10.1007/978-3-642-14295-6_55.

Karp, R.M. and Miller, R.E., 1969. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2):147–195. doi:10.1016/S0022-0000(69)80011-5.

Kosaraju, S.R., 1982. Decidability of reachability in vector addition systems. In *STOC'82*, *14th Symposium on Theory of Computing*, pages 267–281. ACM Press. doi:10.1145/800070.802201.

Leroux, J., 2011. Vector addition system reachability problem: a short self-contained proof. In *POPL 2011*, *38th Annual Symposium on Principles of Programming Languages*, pages 307–316. ACM Press. doi:10.1145/1926385.1926421.

Mayr, E.W., 1981. An algorithm for the general Petri net reachability problem. In *STOC'81*, *13th Symposium on Theory of Computing*, pages 238–246. ACM Press. doi:10.1145/800076.802477.

Rackoff, C., 1978. The covering and boundedness problems for vector addition systems. *Theoretical Computer Science*, 6(2):223–231. doi:10.1016/0304-3975(78)90036-1.

Rosier, L.E. and Yen, H.C., 1986. A multiparameter analysis of the boundedness problem for vector addition systems. *Journal of Computer and System Sciences*, 32(1):105–135. doi:10.1016/0022-0000(86)90006-1.

Valk, R. and Vidal-Naquet, G., 1981. Petri nets and regular languages. *Journal of Computer and System Sciences*, 23(3):299–325. doi:10.1016/0022-0000(81)90067-2.

Weispfenning, V., 1990. The complexity of almost linear Diophantine problems. *Journal of Symbolic Computation*, 10(5):395–403. doi:10.1016/S0747-7171(08)80051-X.

Yen, H.C., 1992. A unified approach for deciding the existence of certain Petri net paths. *Information and Computation*, 96(1):119–137. doi:10.1016/0890-5401(92)90059-O.

A Omitted Proofs

A.1 Proof of Lemma 2.4

Lemma A.1. *Let $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a k-VAS and $\mathcal{C}$ a k-admissible partial cover of $\mathcal{S}$. Then $\mathcal{C} \preccurlyeq C(\mathcal{S})$.*

Proof. Let $\mathcal{C} = \langle S, \rightarrow, \ell, s_0 \rangle$ be a k-admissible partial cover of $\mathcal{S}$ and $C(\mathcal{S}) = \langle S', \rightarrow_C, \ell', s'_0 \rangle$ its CCG. Let us show that

Claim A.1.1. If $s_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n} s_n$ in $\mathcal{C}$, then there exists s'_n in S' s.t. $s'_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n}_C s'_n$ in $C(\mathcal{S})$ and $\ell(s_n) \leq \ell'(s'_n)$.

The claim is trivially true for $n = 0$, and for the induction step, assume $s_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n} s_n \xrightarrow{\mathsf{a}_{n+1}} s_{n+1}$ in $\mathcal{C}$ with $s'_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n}_C s'_n$ and $\ell(s_n) \leq \ell'(s'_n)$ by induction hypothesis. Since $s_n \xrightarrow{\mathsf{a}_{n+1}} s_{n+1}$ and $\ell(s_n) \leq \ell'(s'_n)$, the transition a_{n+1} can also be fired from s'_n, leading to some s'_{n+1}. Now, by definition of k-admissibility (see Definition 2.2), for every $1 \leq j \leq k$, either

1. $\ell(s_{n+1})(j) < \omega$ and thus $\ell'(s'_{n+1})(j) \geq \ell(s_{n+1})(j)$ by monotonicity, or
2. $\ell(s_{n+1})(j) = \omega$ and two cases arise:
   - if $\ell(s_n)(j) = \omega$, then $\ell'(s'_n)(j) = \omega = \ell'(s'_{n+1})(j)$, or
   - there exists a j-antecedent s_i of (s_n, a_{n+1}) on the path $s_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n} s_n$ in $\mathcal{C}$, thus by induction hypothesis on $i \leq n$, $\ell'(s'_i) \geq \ell(s_i)$.

     We proceed by contradiction: assume that $\ell'(s'_{n+1})(j) = (\ell'(s'_n) + \mathsf{a}_{n+1})(j) < \omega$. By definition of a j-antecedent (see (1)),

     $$\ell(s_i)(j) < (\ell(s_n) + \mathsf{a}_{n+1})(j) = (\ell(s_i) + \Delta \mathsf{a}_{i+1} \cdots \mathsf{a}_{n+1})(j) \; , \tag{14}$$

     hence $(\Delta \mathsf{a}_{i+1} \cdots \mathsf{a}_{n+1})(j) > 0$ and

     $$\ell'(s'_i)(j) < (\ell'(s'_i) + \Delta \mathsf{a}_{i+1} \cdots \mathsf{a}_{n+1})(j) = (\ell'(s'_n) + \mathsf{a}_{n+1})(j) < \omega \; . \tag{15}$$

     Furthermore, for every $1 \leq m \leq k$ with $m \neq j$, either $\ell(s_n)(m) = \omega$ and then $\ell'(s'_n)(m) = \omega = \ell'(s'_{n+1})(m)$, or $\ell(s_n)(m) < \omega$ and thus $\ell(s_i)(m) < \omega$ and $(\ell(s_n) + \mathsf{a}_{n+1})(m) = (\ell(s_i) + \Delta \mathsf{a}_{i+1} \cdots \mathsf{a}_{n+1})(m) \geq \ell(s_i)(m)$ implies $(\Delta \mathsf{a}_{i+1} \cdots \mathsf{a}_{n+1})(m) \geq 0$: therefore $\ell'(s'_i)(m) \leq (\ell'(s'_n) + \mathsf{a}_{n+1})(m)$ by monotonicity.

     Thus overall $\ell'(s'_i) \leq \ell'(s'_n) + \mathsf{a}_{n+1}$ and $\ell'(s'_i)(j) < (\ell'(s'_n) + \mathsf{a}_{n+1})(j)$, i.e. s'_i is a j-antecedent for (s'_n, a_{n+1}), in contradiction with $\ell'(s'_{n+1})(j) < \omega$.

Returning to the main proof, let us show that the relation

$$R = \{(s_n, s'_n) \in S \times S' \mid \exists \mathsf{a}_1 \cdots \mathsf{a}_n \in \mathsf{V}^*, \, s_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n} s_n \wedge s'_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n}_C s'_n\} \tag{16}$$

is a monotone simulation between $\mathcal{C}$ and $C(\mathcal{S})$. Indeed,

1. $s_0 \; R \; s'_0$ thus R fulfills Definition 2.3.1, and
2. if $s_n \; R \; s'_n$ then

(a) because $C(\mathcal{S})$ is deterministic, given $\mathsf{a}_1 \cdots \mathsf{a}_n$ there is no choice for s'_n, which verifies $\ell(s_n) \leq \ell'(s'_n)$ by the previous claim, thus R fulfills Definition 2.3.2a, and

(b) if furthermore $s_n \xrightarrow{\mathsf{a}_{n+1}} s_{n+1}$, then by the claim there exists s'_{n+1} s.t. $s'_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_n \mathsf{a}_{n+1}}_C s'_{n+1}$, thus verifying $s_{n+1}\ R\ s'_{n+1}$ by definition of R and $s'_n \xrightarrow{\mathsf{a}_{n+1}}_C s'_{n+1}$ because $C(\mathcal{S})$ is deterministic: R fulfills Definition 2.3.2b. □

A.2 Proof of Proposition 3.1

Proposition A.2. *The VAS model-checking problem for PrCTL$_{\geq}(\mathsf{F})$ is undecidable.*

Proof sketch. We reduce from the VAS model-checking problem for CTL$(\mathsf{F}, \mathsf{X}_\mathsf{a})$, which is shown undecidable by Esparza (1997, Section 4.5) using a reduction from the VAS containment problem. Consider an instance $\langle \mathcal{S}, \varphi \rangle$ of the VAS model-checking problem for CTL$(\mathsf{F}, \mathsf{X}_\mathsf{a})$; we build an instance $\langle \mathcal{S}', \Phi \rangle$ of the PrCTL$_{\geq}(\mathsf{F})$ model-checking problem s.t. $\mathcal{S} \models \varphi$ iff $\mathcal{S}' \models \Phi$. Indeed, let $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a k-VAS with $\mathsf{V} = \{\mathsf{a}_1, \ldots, \mathsf{a}_n\}$, and define a $(k+n)$-VAS $\mathcal{S}'$ that simulates each transition a_j on the first k coordinates and additionally increments coordinate $k+j$. We also define inductively a PrCTL$_{\geq}(\mathsf{F})$ formula $\tau(\varphi)$ from the CTL$(\mathsf{F}, \mathsf{X}_\mathsf{a})$ formula φ, by preserving EF modalities, and by translating relativized "next" subformulæ $\mathsf{EX}_{\mathsf{a}_j}\varphi'$ with a_j in V as $\mathsf{EF}_{\psi_{\mathsf{a}_j}} \tau(\varphi')$ where $\psi_{\mathsf{a}_j}(x_1, \ldots, x_{k'}) \overset{\text{def}}{=} x_{k+j} = 1$. Finally, we need to ensure that the considered partial cover is a partial unfolding of the reachability graph, i.e. that we do not allow ω-values, by defining $\Phi \overset{\text{def}}{=} \tau(\varphi) \wedge \mathsf{AG}\left(\bigwedge_{j=1}^{k+n} \mu(j) < \omega\right)$. □

A.3 Proof of Proposition 3.2

Lemma A.3. *If $\mathcal{S}_1 \preccurlyeq \mathcal{S}_2$ and φ is a PrECTL$_{\geq}(\mathsf{U})$ formula, then $\mathcal{S}_1 \models \varphi$ implies $\mathcal{S}_2 \models \varphi$.*

Proof. By definition of $\mathcal{S}_1 \preccurlyeq \mathcal{S}_2$, there exists a covering simulation $R \subseteq S_1 \times S_2$. First note that the following claim holds by induction on i thanks to Definition 2.3.2b:

Claim A.3.1. If $s\ R\ s'$ and $\pi = q_0 \xrightarrow{\mathsf{a}_1} q_1 \xrightarrow{\mathsf{a}_2} \cdots$ is a path in *Paths*(s), then there exists a path $\pi' = q'_0 \xrightarrow{\mathsf{a}_1} q'_1 \xrightarrow{\mathsf{a}_2} \cdots$ in *Paths*(s') s.t. $q_i\ R\ q'_i$ for all i and $|\pi'| \geq |\pi|$.

For the main proof, let us prove by induction on φ that for any $s\ R\ s'$, $s \models \varphi$ implies $s' \models \varphi$, which will yield the lemma by Definition 2.3.1.

For $\top$ and $\bot$ $s \models \top$ and $s' \models \top$, $s \not\models \bot$ and $s' \not\models \bot$.

For a coverability constraint if $s \models \mu(j) \geq c$, then since $\ell_2(s') \geq \ell_1(s) \geq c$ by Definition 2.3.2a, $s' \models \mu(j) \geq c$.

For $\varphi \vee \varphi'$ or $\varphi \wedge \varphi'$ the result holds by ind. hyp.

For $\mathsf{E}(\varphi\ \mathsf{U}_\psi\ \varphi')$ if $s \models \mathsf{E}(\varphi\ \mathsf{U}_\psi\ \varphi')$, i.e. if there exists a path $\pi = q_0 \xrightarrow{\mathsf{a}_1} q_1 \xrightarrow{\mathsf{a}_2} \cdots$ in $\mathit{Paths}(s)$ and an index $n \le |\pi|$, s.t. PA $\models \psi(\Delta \mathsf{a}_1 \cdots \mathsf{a}_n)$, $q_n \models \varphi'$, and for all $0 \le m < n$, $q_m \models \varphi$, then by the claim, there exists a path $\pi' = q'_1 \xrightarrow{\mathsf{a}_1} q'_2 \xrightarrow{\mathsf{a}_2} \cdots$ in $\mathit{Paths}(s')$ s.t. $q_i\ R\ q'_i$ for all i and $|\pi'| \ge |\pi|$. In particular for $i = n \le |\pi| \le |\pi'|$, by ind. hyp. $q'_n \models \varphi'$, and for all $0 \le i = m < n$, by ind. hyp. $q'_m \models \varphi$. All in all, $s' \models \mathsf{E}(\varphi\ \mathsf{U}_\psi\ \varphi')$. □

Corollary A.4. *Let $\mathcal{S} = \langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a k-VAS and φ a k-formula of PrECTL$_\ge(\mathsf{U}, \mathsf{X})$. Then $\mathcal{S} \models \varphi$ iff $C(\mathcal{S}) \models \varphi$.*

Proof. First assume $\mathcal{S} \not\models \varphi$. By definition, this means that for any k-admissible partial cover $\mathcal{C}$ of $\mathcal{S}$, $\mathcal{C} \not\models \varphi$. Since $C(\mathcal{S})$ is a k-admissible partial cover of $\mathcal{S}$, $C(\mathcal{S}) \not\models \varphi$. Conversely, assume $\mathcal{S} \models \varphi$. By definition, there exists a k-admissible partial cover $\mathcal{C}$ of $\mathcal{S}$ s.t. $\mathcal{C} \models \varphi$. By Lemma 2.4, $\mathcal{C} \preccurlyeq C(\mathcal{S})$, and by Lemma A.3, $C(\mathcal{S}) \models \varphi$. □

By Corollary A.4, the VAS model-checking problem for PrECTL$_\ge(\mathsf{U})$ reduces to the model-checking problem on a particular, finite LTS. As expected, this is a decidable problem:

Lemma A.5. *Let $k \ge 1$, $\mathcal{S} = \langle S, \rightarrow, \ell, s_{init} \rangle$ be a finite LTS, and φ a k-formula of PrCTL$_\ge(\mathsf{U})$. Then whether $\mathcal{S} \models \varphi$ is decidable in nondeterministic polynomial time in $|\mathcal{S}|$ and $|\varphi|$.*

Proof. The decision procedure is an extension of the classical dynamic algorithm for CTL that computes the *satisfaction set* $[\![\varphi']\!]$ for every subformula φ' of φ: for a PrCTL$_\ge$ formula φ', $[\![\varphi']\!] \stackrel{\text{def}}{=} \{s \in S \mid s \models \varphi'\}$. We show that these satisfaction sets can be computed in a finite LTS, and the decision problem then reduces to checking whether $s_{\text{init}} \in [\![\varphi]\!]$.

Write $\mathsf{V} = \{\mathsf{a} \in \mathbb{Z}^k \mid \exists s, s' \in S, s \xrightarrow{\mathsf{a}} s'\}$; V is a finite set $\{\mathsf{a}_1, \dots, \mathsf{a}_n\}$ since $\mathcal{S}$ is finite. Let us first prove the following:

Claim A.5.1. Let $X, Y \subseteq S$ and ψ be a QFP formula with k free variables. Then

$$\begin{aligned}\text{Pre}_{\psi,Y}(X) \stackrel{\text{def}}{=} \{&s_0 \in S \mid \exists s' \in X, \exists m \ge 0, \exists \mathsf{a}_1, \dots, \mathsf{a}_m \in \mathbb{Z}^k,\\ &s_0 \xrightarrow{\mathsf{a}_1} s_1 \cdots s_{m-1} \xrightarrow{\mathsf{a}_m} s' \wedge \text{PA} \models \psi(\Delta \mathsf{a}_1 \cdots \mathsf{a}_m) \wedge \forall i < m, s_i \in Y\}\end{aligned}$$

is effectively computable.

The claim is an easy consequence of Parikh's Theorem: for every s_0 in S, we define the finite automaton $\mathcal{A} = \langle X \cup Y, \mathsf{V}, \delta, \{s_0\}, X \rangle$ with s_0 as unique initial state, $\delta = \rightarrow\ \cap\ (Y \times \mathsf{V} \times (X \cup Y))$ as set of transitions, and X as set of final states. Accepting runs $s_0 \xrightarrow{\mathsf{a}_1} s_1 \cdots s_{m-1} \xrightarrow{\mathsf{a}_m} s'$ in $\mathcal{A}$ verify $s' \in X$ and $\forall i < m$, $s_i \in Y$.

The language $L(\mathcal{A})$ has a semilinear *Parikh image*, which can be described by an existential Presburger formula $\Psi(y_1, \dots, y_n)$ verifying PA $\models \Psi(\mathsf{y})$ for a vector y in $\mathbb{N}^n$ iff there exists an accepting run $s_0 \xrightarrow{\mathsf{a}_1 \cdots \mathsf{a}_m} s'$ in $\mathcal{A}$ with a_i occurring exactly $\mathsf{y}(i)$ times in the string $\mathsf{a}_1 \cdots \mathsf{a}_m$ for every $1 \le i \le n$—see (Verma et al., 2005) for a polynomial-time construction of Ψ from $\mathcal{S}$. Thus a state s_0 belongs to $\text{Pre}_{\psi,Y}(X)$ iff

$$\text{PA} \models \exists y_1, \dots, \exists y_n, \bigwedge_{i=1}^{n} y_i \ge 0 \wedge \Psi(y_1, \dots, y_n) \wedge \psi\left(\sum_{i=1}^{n} \mathsf{a}_i(1) \cdot y_i, \dots, \sum_{i=1}^{n} \mathsf{a}_i(k) \cdot y_i\right)$$

which is decidable in NPTime since this is an existential formula of Presburger Arithmetic.

Returning to the main proof, we merely need to define $[\![\varphi]\!]$ by induction on φ:

$$\begin{aligned}
[\![\top]\!] &\stackrel{\text{def}}{=} S\\
[\![\neg\varphi]\!] &\stackrel{\text{def}}{=} S\backslash[\![\varphi]\!]\\
[\![\varphi \vee \varphi']\!] &\stackrel{\text{def}}{=} [\![\varphi]\!] \cup [\![\varphi']\!]\\
[\![\mathsf{E}(\varphi\ \mathsf{U}_\psi\ \varphi')]\!] &\stackrel{\text{def}}{=} \mathrm{Pre}_{\psi,[\![\varphi]\!]}([\![\varphi']\!])\\
[\![\mu(j) \geq c]\!] &\stackrel{\text{def}}{=} \{s \in S \mid \ell(s)(j) \geq c\}\ .
\end{aligned}$$

□

As a direct consequence of Corollary A.4, of the finiteness of the canonical coverability graph, and of Lemma A.5, we conclude:

Proposition A.6. *The VAS model-checking problem for PrECTL$_\geq$(U) is decidable in nondeterministic polynomial time in $|C(\mathcal{S})|$ and $|\varphi|$.*

A.4 Proof of Proposition 4.1

Proposition A.7. *The satisfiability problem for PrECTL$_\geq$(F) is decidable in* NPTime.

Proof sketch. Let φ be a k-formula of PrECTL$_\geq$(F). Let V be the positive and negative canonical base: $\mathsf{V} = \{\mathsf{e}_j, -\mathsf{e}_j \mid 1 \leq j \leq k\}$ where e_j is the unit vector with $\mathsf{e}_j(j) = 1$ and $\mathsf{e}_j(i) = 0$ if $i \neq j$. For any x_0 in $\mathbb{N}^k$, $\langle \mathsf{V}, \mathsf{x}_0\rangle$ is a k-VAS. Introducing an ω value in coordinate j in order to satisfy a $\mu(j) \geq \omega$ constraint is always possible by firing e_j and $-\mathsf{e}_j$ in sequence. Finite coverability constraints of form $\mu(i) \geq c$ are satisfiable by choosing a high enough x_0. Thus coverability constraints are *always satisfiable*. Finally, satisfying QFP constraints ψ on paths for EF_ψ modalities is done by finding a solution to ψ in NPTime, and if there exists one, playing the corresponding sequence of transitions. To sum up, φ is satisfiable iff all its Presburger formulæ are satisfiable. □

A.5 Proof of Proposition 4.2

Proposition A.8. *Let φ be a k-formula of PrECTL$_\geq$(F). Whether φ is a k-formula of iPrECTL$_\geq$(F) is decidable in* NPTime.

Proof. Let φ be a k-formula of PrECTL$_\geq$(F). We are going to compile the constraints on any tree-shaped model of φ into Presburger arithmetic.

Consider a modal subformula $\mathsf{EF}_\psi\varphi'$ and a tree-shaped submodel with $s \xrightarrow{u} s'$ s.t. $s' \models \varphi'$ and PA $\models \psi(\Delta u)$ (and thus $s \models \mathsf{EF}_\psi\varphi'$). We associate k-tuples of variables $\bar{x} = \langle \bar{x}(1), \ldots, \bar{x}(k)\rangle$, $\bar{y} = \langle \bar{y}(1), \ldots, \bar{y}(k)\rangle$, and $\bar{\Omega} = \langle \bar{\Omega}(1), \ldots, \bar{\Omega}(k)\rangle$ to each such modal subformula of φ representing the reached label $\ell(s')$, the effect of the last followed sequence of transitions Δu, and the set of coordinates holding an ω value $\{1 \leq j \leq k \mid \ell(s)(j) = \omega\}$ (represented by integers with the "C semantics" that value "1" stands for true and any other value for false), along with a k-tuple of variables $\bar{x}_0$ representing the initial (root) marking $\ell(s_0)$.

We inductively define an existential Presburger formula $\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi')$ for each subformula φ' of φ, carrying information about the root marking ($\bar{x}_0$) and the previous marking ($\bar{x}$ and $\bar{\Omega}$):

$$\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \top) \overset{\text{def}}{=} \top \tag{17}$$

$$\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \bot) \overset{\text{def}}{=} \bot \tag{18}$$

$$\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi_1 \vee \varphi_2) \overset{\text{def}}{=} \tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi_1) \vee \tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi_2) \tag{19}$$

$$\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi_2 \wedge \varphi_2) \overset{\text{def}}{=} \tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi_1) \wedge \tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi_2) \tag{20}$$

$$\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \mu(j) \geq c) \overset{\text{def}}{=} \begin{cases} \bar{\Omega}(j) = 1 & \text{if } c = \omega \\ \top & \text{otherwise} \end{cases} \tag{21}$$

$$\tau(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi' = \mathsf{EF}_\psi \varphi'') \overset{\text{def}}{=} \begin{cases} \exists \bar{x}' \bar{\Omega}' . \rho(\bar{\Omega}, \bar{\Omega}') \wedge \tau'(\bar{x}_0, \bar{x}, \bar{x}', \bar{\Omega}', \varphi') & \text{if } \varphi'' \text{ is a CC (13)} \\ \exists \bar{x}' \bar{\Omega}' . \rho(\bar{\Omega}, \bar{\Omega}') \wedge \tau''(\bar{x}_0, \bar{x}, \bar{x}', \bar{\Omega}', \varphi') & \text{otherwise} \end{cases} \tag{22}$$

$$\begin{aligned} \tau'(\bar{x}_0, \bar{x}, \bar{x}', \bar{\Omega}, \varphi') \overset{\text{def}}{=} & (\exists j . 1 \leq j \wedge j \leq k \wedge \bar{\Omega}(j) \neq 1 \wedge \bar{x}'(j) < \bar{x}_0(j)) \\ & \wedge \tau''(\bar{x}_0, \bar{x}, \bar{\Omega}, \varphi') \end{aligned} \tag{23}$$

$$\begin{aligned} \tau''(\bar{x}_0, \bar{x}, \bar{x'}, \bar{\Omega}, \varphi' = \mathsf{EF}_\psi \varphi'') \overset{\text{def}}{=} & \exists \bar{y} . \tau(\bar{x}_0, \bar{x}', \bar{\Omega}', \varphi'') \wedge \psi(\bar{y}) \\ & \wedge \left(\bigwedge_{1 \leq j \leq k} \bar{\Omega}(j) \neq 1 \implies \bar{y}(j) = \bar{x}'(j) - \bar{x}(j) \right) \end{aligned} \tag{24}$$

$$\rho(\bar{\Omega}, \bar{\Omega}') \overset{\text{def}}{=} \bigwedge_{j=1}^{k} \bar{\Omega}(j) = 1 \implies \bar{\Omega}'(j) \; . \tag{25}$$

Hence for each $\varphi' = \mathsf{EF}_\psi \varphi''$ modal subformula, we guess the reached marking (the $\bar{x}'$ and $\bar{\Omega}'$ variables in (22)) and the effect of the last sequence of transitions Δu (the $\bar{y}$ variables in (24)). The latter is checked against ψ in (24). However some of the $\bar{y}$ variables might be left unrelated to the actual effect of u (which is $\bar{x}' - \bar{x}$) if the coordinate j at hand contains an ω-value, i.e. if $\bar{\Omega}(j) = 1$. Equation (21) checks the consistency of the set of ω-values guessed in (22) with coverability constraints, while (25) ensures that ω-values are propagated in the model. When we reach a leaf, i.e. when we consider a formula $\mathsf{EF}_\psi \gamma$ with γ a CC, we check with (23) whether the formula has decreased on this branch, that is to say, whether there is a place on which no ω value was introduced and the current marking $\bar{x}$ is not greater the that of the root $\bar{x}_0$: thus the constructed Presburger formula checks the existence of a counter-example to the fact that φ is increasing.

Consider the same set of vectors V as in the proof Proposition 4.1; given an appropriate x_0 this set can satisfy any φ. Let

$$\Psi \overset{\text{def}}{=} \exists \bar{x}_0 . \tau(\bar{x}_0, \bar{x}_0, (0)_{1 \leq i \leq k}, \varphi) \; ; \tag{26}$$

Ψ is an existential Presburger formula which is satisfiable iff we can build a k-admissible partial cover of the k-VAS $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ (for an appropriate x_0) satisfying φ but not increasing. We have thus reduced the question of increasingness to existential Presburger satisfaction formula; as Ψ can be constructed in polynomial time, the problem can thus be solved in NPTime. □

A.6 Proof of Lemma 4.3

We prove Lemma 4.3 with refined parameters for the size of formulæ:

Formula Size. We consider several parameters on the size of $\mathrm{PrECTL}_{\geq}(\mathsf{F})$ formulæ φ: its *disjunctive size* $|\varphi|_\vee$, corresponding to its modal size when maximizing over disjunctions, defined inductively by

$$|\top|_\vee \overset{\text{def}}{=} |\bot|_\vee \overset{\text{def}}{=} |\mu(j)\geq c|_\vee \overset{\text{def}}{=} 0 \qquad |\mathsf{EF}_\psi\varphi|_\vee \overset{\text{def}}{=} 1+|\varphi|_\vee$$

$$|\varphi\vee\varphi'|_\vee \overset{\text{def}}{=} \max(|\varphi|_\vee,|\varphi'|_\vee) \qquad |\varphi\wedge\varphi'|_\vee \overset{\text{def}}{=} |\varphi|_\vee+|\varphi'|_\vee$$

its *conjunctive size* $|\varphi|_\wedge$ measuring the maximal number of leaves in a tree-shaped model and defined inductively by

$$|\top|_\wedge \overset{\text{def}}{=} |\bot|_\wedge \overset{\text{def}}{=} |\mu(j)\geq c|_\wedge \overset{\text{def}}{=} 0 \qquad |\mathsf{EF}_\psi\varphi|_\wedge \overset{\text{def}}{=} \begin{cases} 1 & \text{if } \varphi \text{ is a CC (13)} \\ 0 & \text{otherwise} \end{cases}$$

$$|\varphi\vee\varphi'|_\wedge \overset{\text{def}}{=} \max(|\varphi|_\wedge,|\varphi'|_\wedge) \qquad |\varphi\wedge\varphi'|_\wedge \overset{\text{def}}{=} |\varphi|_\wedge+|\varphi'|_\wedge$$

(note that $|\varphi|_\vee \geq |\varphi|_\wedge$ for any formula φ), its maximal *constant size*

$$\|\varphi\| \overset{\text{def}}{=} \|\{c\in\mathbb{N} \mid \exists j, (\mu(j)\geq c)\in \mathrm{sub}(\varphi)\}\|$$

and two measures related to the QFP formulæ ψ appearing in EF_ψ modalities: the *Presburger constant size* $\Pr_c(\varphi)$ defined as the log of the maximal constant (i.e. size of a τ subterm according to (7)) appearing in any QFP formula, and the *Presburger constraint size* $\Pr_m(\varphi)$ defined as the total number of Presburger constraints (i.e. of subterms α according to (7)) appearing in φ. For instance, with formulæ (8)–(11), $|\varphi|_\vee \leq 2$, $|\varphi|_\wedge = 1$, and $\Pr_m(\varphi)\leq k$.

Lemma A.9 (Small Models for Bounded LTS)**.** *Let $\langle\mathsf{V},\mathsf{x}_0\rangle$ be a generalized k-VAS with $k>1$, φ be a $\mathrm{PrECTL}_{\geq}(\mathsf{F})$ formula, and $0\leq i\leq k$ and $r\geq 0$. If there exists an (i,r)-bounded partial cover $\mathcal{C}$ of $\langle\mathsf{V},\mathsf{x}_0\rangle$ s.t. $\mathcal{C}\models\varphi_{|_i}$, then there exists a tree-shaped (i,r)-bounded partial cover $\mathcal{C}'$ of $\langle\mathsf{V},\mathsf{x}_0\rangle$ with $\mathcal{C}'\models\varphi_{|_i}$ and $|\mathcal{C}'|\leq(2^{\|\mathsf{V}\|+\Pr_c(\varphi)}r|\varphi|_\vee)^{(k+|\varphi|_\wedge+\Pr_m(\varphi))^d}$ for some constant d (independent of V, x_0, k, φ, i, and r).*

Proof. As in (Rackoff, 1978, Lemma 4.5) we identify and remove loops (called *i-loops*) in (an unfolding of) $\mathcal{C}$ before reintroducing them in a controlled manner in order to maintain both the satisfaction of Presburger formulæ on paths and the existence of some j-antecedent for every introduced ω-value. These two points are specific to our problem.

To this end, we decompose the unfolding of $\mathcal{C}$ into a tree of individual segments where no ω values are introduced. Figure 2 illustrates this decomposition on a partial cover of the VAS of Figure 1 which models the non-regularity formula (11). The model is decomposed into three segments π_1, π_2, and π_3, along with Presburger constraints inherited from EF_ψ modalities (dashed above) and j-antecedency relations (dashed below).

We find and remove i-loops in each segment individually. Both j-antecedency relations and the Presburger formulæ in modalities are used as Presburger constraints on the number of times each i-loop should appear. The bounds of Papadimitriou (1981) on the size of solutions for linear constraints result in a small number of i-loops having to be reintroduced in order to yield $\mathcal{C}'$. Details follow.

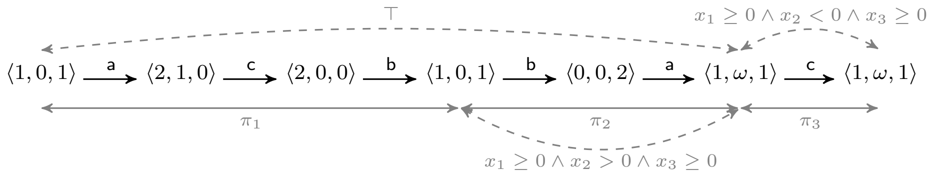
⊤
$x_1 \geq 0 \wedge x_2 < 0 \wedge x_3 \geq 0$
$\langle 1,0,1\rangle \xrightarrow{a} \langle 2,1,0\rangle \xrightarrow{c} \langle 2,0,0\rangle \xrightarrow{b} \langle 1,0,1\rangle \xrightarrow{b} \langle 0,0,2\rangle \xrightarrow{a} \langle 1,\omega,1\rangle \xrightarrow{c} \langle 1,\omega,1\rangle$
π_1
π_2
π_3
$x_1 \geq 0 \wedge x_2 > 0 \wedge x_3 \geq 0$

Figure 2: Decomposition of a model for (11).

Decomposition by EF_ψ Formulæ. The PrECTL$_\geq(\mathsf{F})$ fragment clearly enjoys a *finite tree model property*, in the sense that any k-admissible partial cover $\mathcal{C}$ that models a PrECTL$_\geq(\mathsf{F})$ formula φ can be "unfolded" into a tree-shaped one.

Formally, since

$$\mathsf{EF}_\psi(\varphi \vee \varphi') \equiv (\mathsf{EF}_\psi\varphi) \vee (\mathsf{EF}_\psi\varphi')\ , \tag{27}$$

we can put any PrECTL$_\geq(\mathsf{F})$ formula φ into disjunctive normal form, by pulling all disjunctions to the front, i.e. $\varphi \equiv \bigvee_m \varphi_m$ where each φ_m is disjunction-free. Then by definition $\mathcal{C} \models \varphi$ iff there exists m s.t. $\mathcal{C} \models \varphi_m$, thus we can restrict our attention to disjunction-free formulæ. The unfolding then consists roughly in associating subterms of φ with states of $\mathcal{C}$ and choosing intermediate states for paths verifying $\mathsf{EF}_\psi\varphi'$ formulæ. The latter formulæ decompose $\mathcal{C}'$ into $\leq |\varphi|_\vee$ segments $s \xrightarrow{w} s'$ in $\mathcal{C}$ where $s \models \mathsf{EF}_\psi\varphi'$ thanks to PA $\models \psi(\Delta w)$ and $s' \models \varphi'$.

Example A.10. Consider the CCG $\mathcal{C}$ given in Figure 1 and formula φ_{unreg} given in (11). We have

$$\varphi_{\text{unreg}} \equiv \bigvee_{\substack{I \subseteq \{1,\ldots,k\} \\ I \neq \emptyset}} \ \bigvee_{I \subseteq J \subseteq \{1,\ldots,k\}} \mathsf{EF}\left(\bigwedge_{j \in J} \mu(j) \geq \omega \wedge \mathsf{EF}_{\psi_{I,J}}\top\right) \tag{28}$$

and we can select a subformula satisfied by $\mathcal{C}$ (with $I = J = \{2\}$):

$$\varphi'_{\text{unreg}} \overset{\text{def}}{=} \mathsf{EF}\left(\mu(2) \geq \omega \wedge \mathsf{EF}_{x_1 \geq 0 \wedge x_2 < 0 \wedge x_3 \geq 0}\top\right)\ . \tag{29}$$

In turn, we can unfold $\mathcal{C}$ into the partial cover displayed in Figure 2. The decomposition of this model by EF_ψ subformulæ results in the two segments displayed on top with their respective Presburger constraints.

Decomposition by Antecedents. First observe that there are

$$J \leq k|\varphi|_\wedge \tag{30}$$

pairs (s, a) with a j-antecedent s' in the unfolding of $\mathcal{C}$, because once introduced an ω-value cannot disappear. All in all, this unfolding is split into

$$M \overset{\text{def}}{=} 2J + |\varphi|_\vee \leq 2k|\varphi|_\wedge + |\varphi|_\vee \leq (2k+1)|\varphi|_\vee \tag{31}$$

segments $\pi_1, \ldots, \pi_M$ defined by various extremal points:

1. the $\leq |\varphi|_\vee + 1$ states s, s' witnessing the satisfaction of $\mathsf{EF}_\psi\varphi'$ subformulæ of φ, i.e. with $s \models \mathsf{EF}_\psi\varphi'$ thanks to PA $\models \psi(\Delta w)$ and $s' \models \varphi'$, and
2. the $\leq 2J$ different states s' and s'' corresponding to j-antecedency relations of form $s' \xrightarrow{w} s \xrightarrow{\mathsf{a}} s''$.

No ω-value is introduced within a segment before its last transition.

Let $s' \xrightarrow{w} s \xrightarrow{\mathsf{a}} s''$ be the path witnessing that s' is a j-antecedent of (s, a). We capture this relationship with a QFP formula ψ^j_{z} defined for any z in $\mathbb{N}^k_\omega$ and $j \leq k$ by

$$\psi^j_{\mathsf{z}}(x_1, \ldots, x_k) \overset{\text{def}}{=} x_j > 0 \wedge \bigwedge_{\substack{1 \leq l \leq k \\ \mathsf{z}(l) < \omega}} x_l \geq 0 \; . \tag{32}$$

Indeed, PA $\models \psi^j_{\ell(s'')}(\Delta w \cdot \mathsf{a})$ is then a characterization of j-antecedency. Note that the sequence $w \cdot \mathsf{a}$ might span over several consecutive segments π_p for $1 \leq p \leq M$.

Example A.11. Continuing with the example of Figure 2, an ω-value is introduced in the 6th state with the 1st and 4th states as possible 2-antecedents, where $\psi^2_{\langle 0,0,2\rangle}(x_1, x_2, x_3) \overset{\text{def}}{=} (x_1 \geq 0 \wedge x_2 > 0 \wedge x_3 \geq 0)$, and in each case with PA $\models \psi^2_{\langle 0,0,2\rangle}(\Delta \mathsf{acbba}) = \psi^2_{\langle 0,0,2\rangle}(\Delta \mathsf{ba}) = \psi^2_{\langle 0,0,2\rangle}(\langle 0, 1, 0\rangle)$. Choosing arbitrarily the 4th state as antecedent, we obtain a decomposition into three segments π_1, π_2, and π_3.

The constraints on the segments are then

- PA $\models \top(\Delta \mathsf{acbba})$ (corresponding to the constraint on top of the $\pi_1\pi_2$ segment),
- PA $\models \psi^2_{\langle 0,0,2\rangle}(\Delta \mathsf{ba})$ (corresponding to the constraint below the π_2 segment), and
- PA $\models \psi_{\{2\}}(\Delta \mathsf{c})$ (corresponding to the constraint above the π_3 segment, where $\psi_{\{2\}}(x_1, x_2, x_3)$ is defined in (12) as $x_1 \geq 0 \wedge x_2 < 0 \wedge x_3 \geq 0$).

***i*-Loops Removal.** Next, let u_p be the transition label in $(\mathbb{Z}^k)^*$ of each segment π_p, $1 \leq p \leq M$. We apply the decomposition technique of (Rackoff, 1978, Lemma 4.5) to each u_p: call a factor v of u_p an *i-loop* if $\Delta v(j) = 0$ for each $1 \leq j \leq i$ and $\Delta v'(j) \neq 0$ for some $1 \leq j \leq k$ for any proper factor v' of v, i.e. no proper factor of v is an i-loop. Considering again the example of Figure 2, the sequence acb between the 1st and 4th states is both a 3-loop and a 2-loop, but not a 1-loop because the factor c between the 2nd and 3rd states is a 1-loop.

Rackoff's technique decomposes u_p into a path u'_p and a number of i-loops $(v_n)_n$ in $(\mathbb{Z}^k)^*$ s.t. $|u'_p| \leq (r^k + 1)^2$ and

$$\Delta u_p = \Delta u'_p + \sum_n y_n \cdot \Delta v_n \tag{33}$$

for some constants $(y_n)_n$ each corresponding to the number of times the i-loop v_n is removed. In addition, the set of projections on the first i places of vectors along u'_p is the same as that of u_p, which garantees that i-loops can be reintroduced freely.

Each i-loop v_n obtained this way has length at most $r^i \leq r^k$, thus each coordinate $\Delta v_n(j)$ has absolute value at most $a_{\max} \overset{\text{def}}{=} 2^{\|\mathsf{V}\|} r^k$, thus there are at most $N \overset{\text{def}}{=} (2(2^{\|\mathsf{V}\|} r^k) + 1)^k$ i-loops with different effects. Identifying i-loops having the same effect, we see that (33) only needs N different y_n, while the effect $\Delta u'_p$ is of absolute value at most $b_{\max} \overset{\text{def}}{=} 2^{\|\mathsf{V}\|}(r^k + 1)^2$ on every coordinate.

Reintroducing i-Loops. In order to obtain a partial cover $\mathcal{C}'$ that models φ, we merely need to ensure that both the j-antecedent relations and the Presburger constraints on paths are preserved. Indeed, finite values on the first i coordinates are preserved by i-loop removal, thus the only difficulty is to ensure that ω-values and Presburger constraints are also preserved, so that we obtain a partial cover and preserve constraints of form $\mu(j) \geq \omega$.

We reintroduce i-loops: each of the J j-antecedency constraints translates into verifying a Presburger constraint $\mathrm{PA} \models \psi^j_{\ell(s'')}(\sum_{p \in P} \Delta u_p)$ and each of the $|\varphi|_\vee$ modal subterms $\mathsf{EF}_\psi \varphi'$ into a Presburger constraint $\mathrm{PA} \models \psi(\sum_{p \in P} \Delta u_p)$, each time for some set P of consecutive indices corresponding to the span of the j-antecedent relation or path verifying ψ, and we need to enforce the conjunction of all these $J + |\varphi|_\vee$ constraints. Therefore, we obtain a system of linear constraints in

$$\begin{aligned} n &\overset{\text{def}}{=} (J + |\varphi|_\vee) \cdot N + \mathrm{Pr}_m(\varphi) \\ &\leq (k|\varphi|_\wedge + |\varphi|_\vee) \cdot N + \mathrm{Pr}_m(\varphi) \\ &\leq (k+1)|\varphi|_\vee \cdot N + \mathrm{Pr}_m(\varphi) \\ &= (k+1)|\varphi|_\vee (2(2^{\|\mathsf{V}\|} r^k) + 1)^k + \mathrm{Pr}_m(\varphi) \end{aligned} \tag{34}$$

integer variables (telling how many times each i-loop should be reintroduced)—the $\mathrm{Pr}_m(\varphi)$ term is needed to account for divisibility relations $\tau \equiv_p \tau'$ in QFP formulæ—and

$$m \overset{\text{def}}{=} J \cdot k + \mathrm{Pr}_m(\varphi) \leq k^2 |\varphi|_\wedge + \mathrm{Pr}_m(\varphi) \tag{35}$$

constraints, with variable coefficients $\leq a_{\max} \cdot 2^{\mathrm{Pr}_c(\varphi)}$ in absolute value, and constant coefficients $\leq M \cdot b_{\max} + 2^{\mathrm{Pr}_c(\varphi)} \leq (2k+1)|\varphi|_\vee b_{\max} + 2^{\mathrm{Pr}_c(\varphi)}$ in absolute value. By the results of (Papadimitriou, 1981) (see also (Seshia and Bryant, 2005, Theorem 2)), we deduce a bound of

$$\begin{aligned} &(n + 1 + m)(1 + (2k+1)|\varphi|_\vee b_{\max} + 2^{\mathrm{Pr}_c(\varphi)})(m(a_{\max} + 2^{\mathrm{Pr}_c(\varphi)}))^{2m+3} \\ &\qquad\qquad \leq (2^{\|\mathsf{V}\| + \mathrm{Pr}_c(\varphi)} r |\varphi|_\vee)^{(k + |\varphi|_\wedge + \mathrm{Pr}_m(\varphi))^c} \end{aligned} \tag{36}$$

for some constant c on the solutions of this system, i.e. on the number of times each i-loop should be repeated. Multiplying (36) by the maximal length r^k of an i-loop and adding the sum $M(r^k + 1)^2$ of the lengths of the u'_p segments, we end up with a bound of $(2^{\|\mathsf{V}\| + \mathrm{Pr}_c(\varphi)} r |\varphi|_\vee)^{(k + |\varphi|_\wedge + \mathrm{Pr}_m(\varphi))^d}$ for some constant d on the length of the new partial cover $\mathcal{C}'$. □

A.7 Proof of Lemma 4.4

We prove Lemma 4.4 for a refined version of g that takes formula size into account. Given $\mathsf{V} \subseteq (\mathbb{Z}_\omega)^k$, a k-coverability formula φ, and some $0 \leq i < k$, let

$$g(0) \stackrel{\text{def}}{=} (2^{\|\mathsf{V}\|+\mathrm{Pr}_c(\varphi)} \cdot |\mathsf{V}| \cdot |\varphi|_\vee)^{(k+|\varphi|_\wedge+\mathrm{Pr}_m(\varphi))^d}$$

$$g(i+1) \stackrel{\text{def}}{=} \left(2^{\|\mathsf{V}\|+\mathrm{Pr}_c(\varphi)} \cdot (2^{\|\mathsf{V}\|}g(i) + 2^{\|\varphi\|}) \cdot |\varphi|_\vee\right)^{(k+|\varphi|_\wedge+\mathrm{Pr}_m(\varphi))^d} + 1 + g(i)$$

where d is the constant of Lemma 4.3.

Lemma A.12. *Let $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ be a k-VAS and $\varphi = \mathsf{EF}\varphi'$ be an eventually increasing k-formula. Let $\mathcal{C}$ be an i-admissible partial cover of $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ with $\mathcal{C} \models \varphi_{|_i}$. Then there exists a tree-shaped i-admissible partial cover $\mathcal{C}'$ of $\langle \mathsf{V}, \mathsf{x}_0 \rangle$ s.t. $\mathcal{C}' \models \varphi_{|_i}$ and $|\mathcal{C}'| \leq g(i)$.*

Proof. The proof follows in part (Rackoff, 1978, Lemma 4.6 & 4.7) and is by induction on i.

Base Case $i = 0$. The only requisite of $\varphi_{|_0}$ are Presburger constraints on paths and proper introduction of ω-values. As in the proof of Lemma 4.3, we decompose a model of $\varphi_{|_0}$ into M segments, each labeled by some u_p, $1 \leq p \leq M$, with $\Delta u_p = \sum_{n=1}^{|\mathsf{V}|} y_n \mathsf{a}_n$ for some $(y_n)_n$ where $\mathsf{V} = \{\mathsf{a}_1, \ldots, \mathsf{a}_{|\mathsf{V}|}\}$. The j-antecedent constraints and Presburger constraints result in m linear constraints as in (35) over

$$n \stackrel{\text{def}}{=} (J + |\varphi|_\vee) \cdot |\mathsf{V}| + \mathrm{Pr}_m(\varphi) \leq (k+1)|\varphi|_\vee |\mathsf{V}| + \mathrm{Pr}_m(\varphi) \tag{37}$$

variables with coefficients at most $a_{\max} \stackrel{\text{def}}{=} 2^{\|\mathsf{V}\|+\mathrm{Pr}_c(\varphi)}$ in absolute value and constants at most $b_{\max} \stackrel{\text{def}}{=} 2^{\mathrm{Pr}_c(\varphi)}$, thus by (Papadimitriou, 1981) we can construct a model $\mathcal{C}'$ of size at most

$$(n+1+m)(1+b_{\max})(ma_{\max})^{2m+3} \leq (2^{\|\mathsf{V}\|+\mathrm{Pr}_c(\varphi)} \cdot |\mathsf{V}| \cdot |\varphi|_\vee)^{(k+|\varphi|_\wedge+\mathrm{Pr}_m(\varphi))^d} = g(0)$$

for the constant d of Lemma 4.3.

Induction Step for $i + 1$. Let $\varphi_{|_{i+1}} = \mathsf{EF}\varphi'$ with φ' an increasing formula. We assume wlog. $\mathcal{C}$ to be tree-shaped, with an initial path of form $s_{\text{init}} \to^* s_0$ s.t. $s_0 \models \varphi'$. Set

$$r \stackrel{\text{def}}{=} 2^{\|\mathsf{V}\|}g(i) + 2^{\|\varphi\|}\ , \tag{38}$$

which a high enough value to ensure any model of size $g(i)$ will be unable to decrease a coordinate holding r below the maximal finite constant c appearing in a $\mu(j) \geq c$ subformula of $\varphi_{|_{i+1}}$. Two cases arise:

If $\mathcal{C}$ is $(i + 1, r)$-bounded then by Lemma 4.3 it is of length at most

$$(2^{\|\mathsf{V}\|+\mathrm{Pr}_c(\varphi)} r |\varphi|_\vee)^{(k+|\varphi|_\wedge+\mathrm{Pr}_m(\varphi))^d} = g(i+1)\ .$$

Otherwise there exists some state s' in $\mathcal{C}$ with $r \leq \ell(s')(j) < \omega$ for some j; wlog. we assume this to occur only in $j = i + 1$.

Consider the leaves $s_1, \dots, s_n$ of $\mathcal{C}$. Since φ' is increasing, $\ell(s_l) \geq \ell(s)$ for all $1 \leq l \leq n$. By monotonicity, this means that we can "replay" the entire submodel rooted in s_0 from any of the leaves $s_1, \dots, s_n$, i.e. fire the same sequences of transitions and introduce (if necessary) ω-values at the same points. By performing this operation sequentially on s_1, then on s_2^1 (the leaf corresponding to s_2 in the replay started in s_1), then on s_3^2 (the leaf corresponding to s_3^1 in the replay from s_2^1, where s_3^1 is the leaf corresponding to s_3 in the replay from s_1), ..., we end with a copy of the submodel rooted at s_n^{n-1} s.t. $s_n^{n-1} \models \varphi'$, and $s_{\text{init}} \to^* s_0 \to^* s_1 \to^* s_2^1 \to^* s_3^2 \to^* \cdots s_n^{n-1}$, i.e. we have constructed a model $\mathcal{C}_1$ of $\varphi_{|_{i+1}}$, which is also an $(i+1)$-admissible partial cover of $\langle \mathsf{V}, \mathsf{x}_0 \rangle$.

There are two immediate but crucial properties of $\mathcal{C}_1$:

1. there exists now a first state s' with $r \leq \ell(s')(j) < \omega$ reachable from s_{init}, and it appears somewhere in the segment $s_{\text{init}} \to^* s_n^{n-1}$;
2. any ω-value that appeared in any of the leaves $s_1, \dots, s_n$ is now introduced during the prefix $s_{\text{init}} \to^* s_n^{n-1}$ and its j-antecedency relation also points inside this prefix.

Because of these two properties, we can identify j-antecedency relations that "cross" the s' boundary inside the $s_{\text{init}} \to^* s_n^{n-1}$ prefix. By monotonicity, we can also "replay" the pumping segment (called $w\mathsf{a}$ in (1)) and introduce the ω-value on the second instance only; doing so for all the j-antecedency relations that span over s' (in their order of appearance after s') allows to split the prefix $s_{\text{init}} \to^* s_n^{n-1}$ into two segments $s_{\text{init}} \to^* s'$ and $s' \to^* s_n^{n-1}$ with no j-antecedency relations crossing over s'. Call $\mathcal{C}_2$ this new model of $\varphi_{|_{i+1}}$.

We now treat the prefix $s_{\text{init}} \to^* s'$ and the suffix $s' \to^* s_n^{n-1}$ with the submodel rooted at s_n^{n-1} separately:

- the prefix $s_{\text{init}} \to^* s'$ can in turn be split into $s_{\text{init}} \to^* s \xrightarrow{\mathsf{a}} s'$ with a in V and s the last state with $\ell(s)(j) < r$ or $\ell(j) = \omega$ for all $1 \leq j \leq i+1$. The segment $s_{\text{init}} \to^* s$ is $(i+1, r)$-bounded and verifies the $(i+1)$-formula

$$\varphi'' \stackrel{\text{def}}{=} \mathsf{EF} \bigwedge_{j=1}^{i+1} (\mu(j) \geq \ell(s)(j)) \wedge \bigwedge_{j | \ell(s)(j) = \omega} (\mu(j) \geq \omega) \; . \tag{39}$$

  By Lemma 4.3 we can replace $s_{\text{init}} \to^* s$ by another prefix also verifying φ'' of size at most

$$(2^{\|\mathsf{V}\|} r)^{k^d} \tag{40}$$

  By monotonicity, continuing this model of φ'' with a and the suffix we obtain a model of $\varphi_{|_{i+1}}$.

- the suffix $s' \to^* s_n^{n-1}$ along with the submodel rooted at s_n^{n-1} is in particular an i-admissible model of $\varphi_{|_i}$ for the generalized k-VAS $\langle \mathsf{V}, \ell(s) \rangle$. By induction hypothesis we can replace it with a model of size $g(i)$. Since $\ell(s)(i+1) \geq r$, this new model is also $(i+1)$-admissible and models $\varphi_{_{i+1}}$, as no value on the $(i+1)$th coordinate can drop below the largest constant in φ.

All in all, we have constructed a model $\mathcal{C}'$ of size at most

$$(2^{\|\mathsf{V}\|}r)^{k^d} + 1 + g(i) = \left(2^{\|\mathsf{V}\|}(2^{\|\mathsf{V}\|}g(i) + 2^{\|\varphi\|})\right)^{k^d} \leq g(i+1)\,. \qquad \square$$

A.8 Proof of Theorem 4.5

Theorem A.13 (Complexity of VAS model checking)**.** *The VAS model-checking problem for eiPrECTL$_{\geq}$(*F*) formulæ is* ExpSpace*-complete.*

Proof. The hardness result already holds for place coverability and is due to Lipton (Cardoza et al., 1976). We only need to prove the upper bounds.

Thanks to Lemma 4.4, we know that if a coverability formula φ has a model, then it has one of size is bounded by

$$g(k) \leq (2^{\|\mathsf{V}\|+\|\varphi\|+\mathrm{Pr}_c(\varphi)}|\mathsf{V}||\varphi|_\vee)^{2^{kd'\log_2(k+|\varphi|_\wedge+\mathrm{Pr}_m(\varphi))}} \tag{41}$$

for some constant d' independent of V and φ. We use a non-deterministic algorithm, that guesses and checks a witness on the fly up to length $g(k)$ in space $O((\|\mathsf{V}\| + \|\varphi\| + \mathrm{Pr}_c(\varphi) + \log_2|\mathsf{V}| + \log_2|\varphi|_\vee) \cdot (k + |\varphi|_\wedge + \mathrm{Pr}_m(\varphi)) \cdot 2^{kd'})$, which is polynomial for fixed k and exponential otherwise. Note that the size of the formula φ only influences this bound polynomially. □

B Additional Comments

B.1 Extensions of PrECTL$_{\geq}$(U)

We consider in this section the PrECTL$_{\geq}$(G) fragment, and a variant of PrECTL$_{\geq}$(U) with “until” refined by *two* QFP formulæ.

“Globally” Modalities. We use the natural semantics of G as a dual modality of F:

$$\begin{aligned} s \models \mathsf{EG}_\psi\varphi \qquad & \text{iff } \exists\pi = s_0 \xrightarrow{\mathsf{a}_1} s_1 \xrightarrow{\mathsf{a}_2} \cdots \in \mathit{Paths}(s),\\ & \qquad \forall n \leq |\pi|,\ \mathrm{PA} \models \psi(\Delta\mathsf{a}_1\cdots\mathsf{a}_n) \text{ implies } s_n \models \varphi\,. \end{aligned}$$

This EG modality is not very useful with our partial cover semantics, because we have no control on the length of paths (it often suffices to “cut” a branch in order to satisfy a EG modality). However, if we look at satisfaction on a *particular* partial cover, things change:

Proposition B.1 (Undecidability of CCG Model-Checking)**.** *Let $\mathcal{S} = \langle\mathsf{V},\mathsf{x}_0\rangle$ be a k-VAS and φ a k-formula of PrECTL$_{\geq}$(*G*). It is undecidable whether $C(\mathcal{S}) \models \varphi$.*

Proof sketch. We reduce an instance $\langle\mathcal{M}\rangle$ of the halting problem in 2-counter deterministic Minsky machines to an instance $\langle\mathcal{S},\varphi\rangle$ of the CCG model-checking problem. The construction of $\mathcal{S}$ is classical, using nondeterminism to simulate “q: if $c = 0$ then goto q' else $c \leftarrow c - 1$; goto q''” instructions. This VAS allows many incorrect runs in addition to a single *honest* run that corresponds to the unique run of $\mathcal{M}$. The task of φ is thus to filter out dishonest runs in $C(\mathcal{S})$ and only leave the honest one, and also to test whether the honest run halts. Let

$$\varphi \stackrel{\text{def}}{=} \mathsf{EG}_{\psi_{\neg\text{honest}\vee\text{halt}}} \bot \; . \tag{42}$$

A run $\pi = s_0 \xrightarrow{\mathsf{a}_1} s_1 \xrightarrow{\mathsf{a}_2} \cdots$ satisfying φ has to continuously ensure that $\text{PA} \not\models \psi_{\neg\text{honest}\vee\text{halt}}(\Delta\mathsf{a}_1 \cdots \mathsf{a}_n)$. As should be clear from its name, $\psi_{\neg\text{honest}\vee\text{halt}}$ holds if the run is dishonest or halts, so that $C(\mathcal{S}) \models \varphi$ iff $\mathcal{M}$ does not halt.

Assuming $\mathcal{S}$ to be a $(2|Q|+2)$-VAS coding the states of $\mathcal{M}$ in its first $2|Q|$ coordinates and the two counters in the last two coordinates, and coordinate $q \in Q_t$ to denote that an "if branch" has just been chosen (which should imply that the counter c_q holds zero), this can be checked by defining

$$\begin{aligned} \psi_{\neg\text{honest}\vee\text{halt}} \stackrel{\text{def}}{=} & \bigvee_{c=1}^{2} x_{2|Q|+c} < 0 && \text{(negative counter value)} \\ & \vee \bigvee_{q \in Q_t} x_q \geq 1 \wedge x_{c_q} > 0 && \text{("if branch" when } c_q \neq 0) \\ & \vee x_{2q_f} \geq 1 \; . && \text{(halt state)} \end{aligned}$$

Observe that this proof does not hold if we consider any k-admissible partial cover instead of the CCG: the cover could simply stop in the initial state and verify φ even if $\mathcal{M}$ did halt. □

"Until" Modalities with Two Presburger Formulæ. The semantics of EG_ψ lead rather naturally to an extension of $\text{PrCTL}_{\geq}(\mathsf{U})$ where we also control what happens along the way of the "until":

$$\begin{aligned} s \models \mathsf{E}(\varphi \,\mathsf{U}_{\psi,\psi'}\, \varphi') \quad & \text{iff } \exists \pi = s_0 \xrightarrow{\mathsf{a}_1} s_1 \xrightarrow{\mathsf{a}_2} \cdots \in \mathit{Paths}(s),\, \exists n \leq |\pi|, \\ & \quad \text{PA} \models \psi'(\Delta\mathsf{a}_1 \cdots \mathsf{a}_n),\, s_n \models \varphi',\text{ and} \\ & \quad \forall m < n,\, \text{PA} \models \psi(\Delta\mathsf{a}_1 \cdots \mathsf{a}_m) \text{ implies } s_m \models \varphi \; . \end{aligned}$$

The "until" modality of the paper can then defined as $\mathsf{E}(\varphi \,\mathsf{U}_\psi\, \varphi') \stackrel{\text{def}}{=} \mathsf{E}(\varphi \,\mathsf{U}_{\top,\psi}\, \varphi')$. Let us call the resulting existential fragment $\text{PrECTL}_{\geq}(\mathsf{U}_2)$; it is easily seen to have an undecidable VAS model-checking problem:

Proposition B.2. *The VAS model-checking problem for $\mathit{PrECTL}_{\geq}(\mathsf{U}_2)$ is undecidable.*

Proof sketch. As in the proof sketch for Proposition B.1, we reduce from the halting problem of deterministic 2-counter Minsky machines. In fact we keep the same construction for the VAS $\mathcal{S}$ and only slightly modify the formula:

$$\varphi \stackrel{\text{def}}{=} \mathsf{E}(\bot \,\mathsf{U}_{\psi_{\neg\text{honest}},\psi_{\text{halt}}}\, \top) \; . \tag{43}$$

We leave the definition of $\psi_{\neg\text{honest}}$ and ψ_{halt} to the reader's imagination, and conclude with the fact that $\mathcal{S} \models \varphi$ iff $\mathcal{M}$ halts. □

B.2 More Coverability-Like Properties

We present in this section a few more properties of vector addition systems testable in ExpSpace. We already gave eiPrECTL$_{\geq}(\mathsf{F})$ formulæ for coverability, boundedness, place boundedness, and regularity in (8)–(11). We found more examples considered by Yen (1992, Section 4), Atig and Habermehl (2009, Section 6.1), and Demri (2010, Section 3.3).

1. *Nondeterminism* is a variant of coverability and asks whether two different transitions a and a' can be fired simultaneously. Define the vector of $\mathbb{N}^k$ x_a by $\mathsf{x}_\mathsf{a}(j) = -\mathsf{a}(j)$ if $\mathsf{a}(j) < 0$ and $\mathsf{x}_\mathsf{a}(j) = 0$ otherwise, and take the (pointwise) least upper bound $\mathsf{x}_\mathsf{a} \sqcup \mathsf{x}_{\mathsf{a}'}$: nondeterminism reduces to coverability of $\mathsf{x}_\mathsf{a} \sqcup \mathsf{x}_{\mathsf{a}'}$ for some $\mathsf{a} \neq \mathsf{a}'$:
$$\varphi_{\text{nondet}} \overset{\text{def}}{=} \mathsf{EF} \bigvee_{\mathsf{a}\neq\mathsf{a}'\in\mathsf{V}} \bigwedge_{j=1}^{k} \mu(j) \geq (\mathsf{x}_\mathsf{a} \sqcup \mathsf{x}_{\mathsf{a}'})(j)\ . \tag{44}$$

2. *Repeated control-state reachability* (Habermehl, 1997) is used to model-check ω-regular properties. Using an encoding of the set of states Q using $\lceil \log_2 Q \rceil$ additional counters and an extra counter at index t incremented with every transition, this property is a form of *repeated coverability* for some vector x, and captured by
$$\varphi_{\text{rep-cov},\mathsf{x}} \overset{\text{def}}{=} \mathsf{EF} \left((\bigwedge_{j=1}^{k} \mu(j) \geq \mathsf{x}_j) \wedge \mathsf{EF}_{\psi_{\text{rep-cov}}} \top \right) \tag{45}$$
where
$$\psi_{\text{rep-cov}}(x_1, \ldots, x_k) \overset{\text{def}}{=} x_t > 0 \wedge \bigwedge_{j\neq t} x_j \geq 0\ . \tag{46}$$
Indeed, if there exists an infinite run in $R(\mathcal{S})$ where x is covered infinitely often, we can consider the infinite sequence $\mathsf{x}_0, \mathsf{x}_1, \ldots$ of configurations $\geq \mathsf{x}$ in this run; by Dickson's Lemma there exists two indices $i_1 < i_2$ in this sequence s.t. $\mathsf{x}_{i_1} \leq \mathsf{x}_{i_2}$ thus the corresponding factor between i_1 and i_2 in the run verifies the $\psi_{\text{rep-cov}}$ condition. Conversely, if $\varphi_{\text{rep-cov},\mathsf{x}}$ holds, then there exists a run covering x infinitely often by monotonicity.

3. *Simultaneous unboundedness* (Demri, 2010) tests whether a subset I of $\{1, \ldots, k\}$ can be simultaneously unbounded. This is very simply captured by
$$\varphi_{\text{sunb},I} \overset{\text{def}}{=} \mathsf{EF} \bigwedge_{j\in I} \mu(j) \geq \omega\ . \tag{47}$$

4. *Trace boundedness* (Chambart et al., 2011) checks whether the language of a VAS is a *bounded language* according to Ginsburg and Spanier (1964)'s definition. Trace unboundedness can be checked by
$$\begin{aligned}\varphi_{\text{tunb}} \overset{\text{def}}{=} \mathsf{EF} \bigvee_{\mathsf{a}\neq\mathsf{b}\in\mathsf{V}} \bigvee_{I\subseteq\{1,\ldots,k\}} \bigwedge_{j\in I} \mu(j) \geq \omega \\ \wedge (\mathsf{EX}_\mathsf{a}\mathsf{EF}_{\psi_{I,\mathsf{a}}}\top) \wedge (\mathsf{EX}_\mathsf{b}\mathsf{EF}_{\psi_{I,\mathsf{b}}}\top)\end{aligned} \tag{48}$$

where EX_{a} was defined in the proof of Proposition 3.1, and $\psi_{I,\mathsf{a}}$ is defined for all a in $\mathbb{Z}^k$ and $I \subseteq \{1, \ldots, k\}$ by

$$\psi_{I,\mathsf{a}}(x_1, \ldots, x_k) \stackrel{\text{def}}{=} \bigwedge_{j \notin I} x_j \geq -\mathsf{a}(j) \ . \tag{49}$$

It checks for the existence of two loops in the coverability graph, starting with two different initial transitions on a and b (see (Chambart et al., 2011, Proposition 4)).

Demri also shows that there is a LogSpace reduction of the *strong promptness detection* problem to the complement of the simultaneous unboundedness problem (Demri, 2010, Lemma 3.4); in the same way, *reversal-boundedness* (Finkel and Sangnier, 2008) reduces to place boundedness.

It is worth noting that in all our examples the various parameters on formula sizes remained small: $|\varphi|_\vee \leq 5$, $|\varphi|_\wedge \leq 2$, $\|\varphi\| \leq \|\mathsf{V}\|$, $\mathrm{Pr}_c(\varphi) \leq \|\mathsf{V}\|$, and $\mathrm{Pr}_m(\varphi) \leq k$.

Additional References

Ginsburg, S. and Spanier, E.H., 1964. Bounded Algol-like languages. *Transactions of the American Mathematical Society*, 113(2):333–368. doi:10.2307/1994067.

Papadimitriou, C.H., 1981. On the complexity of integer programming. *Journal of the ACM*, 28(4):765–768. doi:10.1145/322276.322287.

Parikh, R.J., 1966. On context-free languages. *Journal of the ACM*, 13(4):570–581. doi:10.1145/321356.321364.

Seshia, S.A. and Bryant, R.E., 2005. Deciding quantifier-free Presburger formulas using parametrized solution bounds. *Logical Methods in Computer Science*, 1(2:6):1–26. doi:10.2168/LMCS-1(2:6)2005.

Verma, K.N., Seidl, H., and Schwentick, T., 2005. On the complexity of equational Horn clauses. In Nieuwenhuis, R., editor, *CADE-20, 20th International Conference on Automated Deduction*, volume 3632 of *Lecture Notes in Computer Science*, pages 337–352. Springer. doi:10.1007/11532231_25.