A Relational Trace Logic for Vector Addition Systems with Application to Context-Freeness

Jérôme Leroux, M Praveen, Grégoire Sutre

A Relational Trace Logic for Vector Addition Systems with Application to Context-Freeness[*]

Jérôme Leroux, M. Praveen, and Grégoire Sutre

Univ. Bordeaux & CNRS, LaBRI, UMR 5800, Talence, France

Abstract. We introduce a logic for specifying trace properties of vector addition systems (VAS). This logic can express linear relations among pumping segments occurring in a trace. Given a VAS and a formula in the logic, we investigate the question whether the VAS contains a trace satisfying the formula. Our main contribution is an exponential space upper bound for this problem. The proof is based on a small model property for the logic. Compared to similar logics that are solvable in exponential space, a distinguishing feature of our logic is its ability to express non-context-freeness of the trace language of a VAS. This allows us to show that the context-freeness problem for VAS, whose complexity was not established so far, is ExpSpace-complete.

1 Introduction

Vector addition systems (VAS), or equivalently Petri nets, are well-studied for the modeling and analysis of concurrent systems. Despite their fairly large expressive power, many verification problems for VAS are decidable: coverability, boundedness, reachability, liveness, regularity, etc. [4]. The complexity of many of these decision problems has also been established.

Known decidable problems for VAS can be broadly classified into two classes. The first one, that we call $\mathcal{C}_{\mathrm{RP}}$, consists of those problems that are equivalent to the reachability problem in terms of computational complexity. Examples of problems in $\mathcal{C}_{\mathrm{RP}}$ include reachability, liveness, model checking some fragments of linear temporal logic, etc. The exact complexity of these problems is still open. The best known lower bound is ExpSpace-hardness [9]. There is no known upper bound, except that these problems are decidable [10, 6].

The second class of problems, that we call $\mathcal{C}_{\mathrm{KM}}$, are those that can be decided using the Karp & Miller coverability graph [5]. Examples of problems in $\mathcal{C}_{\mathrm{KM}}$ include coverability, boundedness, regularity, etc. In general, the size of the coverability graph can be Ackermann in the size of the VAS. Still, most of the problems in $\mathcal{C}_{\mathrm{KM}}$ can be decided in exponential space, by applying a technique introduced by Rackoff [13], or extending this technique [1–3].

The question whether the set of traces of a VAS is context-free is also in the class $\mathcal{C}_{\mathrm{KM}}$. It was shown to be decidable by Schwer in [14], based on the coverability graph. Recently, we showed in [8] that non-context-freeness of the set of

---

traces can always be witnessed by a regular bounded language $u_1\sigma_1^* \cdots u_k\sigma_k^*$ that has a non-context-free intersection with the set of traces. Like context-freeness, for most of the properties in $\mathcal{C}_{\mathrm{KM}}$, we can find violating witnesses that are given by regular bounded languages of the form $u_1\sigma_1^* \cdots u_k\sigma_k^*$. Equivalently, we consider, in this paper, witnesses that are given as traces satisfying an iterability condition. Intuitively, a *self-covering sequence* is a trace $u_1\sigma_1 \cdots u_k\sigma_k$ such that, for every $n \geq 0$, there is a trace in $u_1\sigma_1^{\geq n} \cdots u_k\sigma_k^{\geq n}$. The words $\sigma_1, \ldots, \sigma_k$ are called *pumping segments*, as they can be iterated. To witness the violation of a given property, the displacements of the pumping segments are required to additionally satisfy some linear relations depending on the property under consideration.

Contributions. We introduce a relational logic over self-covering sequences. This logic can express positive Boolean combinations of linear relations among the displacements of pumping segments. We show that many properties in $\mathcal{C}_{\mathrm{KM}}$ can be expressed by the logic, in particular: coverability, boundedness, simultaneous unboundedness, regularity, and recurrence. Our main technical result is a small model property: we show that if there is a self-covering sequence satisfying a formula of the logic, then there is one of size at most doubly-exponential. This gives an exponential space upper bound for the problem whether a given VAS satisfies a given formula. Then, we focus on the context-freeness problem. We prove that the presence of self-covering sequences witnessing non-context-freeness can be expressed in our logic. We thus derive an exponential space upper bound for the context-freeness problem, whose complexity was still open.

Extensions of the technique introduced by Rackoff [13] are not enough for proving the small model property mentioned above. Our approach is based on reversibility domains [7]. The reversibility domain of an action is the set of configurations from which the effect of the action can be canceled by a word of actions. A doubly exponential bound on the minimal elements of these upward closed sets is derived in [7]. This result is central in our approach.

Related work. Other logics that can be checked in exponential space have been investigated before. The fragment of Yen's path logic [17] introduced by Atig and Habermehl [1], the fragment of computational tree logic by Blockelet and Schmitz [2] and the generalized unboundedness properties of Demri [3] are in this category. All of these impose conditions that are incompatible with context-freeness. We provide a more detailed comparison with related work at the end of the paper.

Outline. We recall in Section 2 some basic notions on VAS and define self-covering sequences. Section 3 introduces our relational trace logic. We show in Section 4 that many classical problems on VAS can be expressed in this logic. We establish in Sections 5, 6, and 7 the exponential space complexity of the problem whether a given VAS satisfies a given formula. Section 8 applies the results of the previous sections to the context-freeness problem for VAS. We conclude in Section 9 with a detailed comparison with related work.

2 Vector Addition Systems

We let $\mathbb{N}$ and $\mathbb{Z}$ denote the sets of *natural numbers* and *integers* respectively. For $\mathbb{X} \in \{\mathbb{N}, \mathbb{Z}\}$ and $\# \in \{<, \leq, \geq, >\}$, we write $\mathbb{X}_{\#0} = \{x \in \mathbb{X} \mid x \# 0\}$. Vectors and sets of vectors are typeset in bold face. The *ith component* of a vector $\boldsymbol{v}$ is written $\boldsymbol{v}(i)$. The *zero vector* is written $\boldsymbol{0}$. We let $\boldsymbol{e}_i$ denote the *ith unit vector*, defined by $\boldsymbol{e}_i(i) = 1$ and $\boldsymbol{e}_i(j) = 0$ for every index $j \neq i$. Given a vector $\boldsymbol{v}$, we write $\|\boldsymbol{v}\|^+, \|\boldsymbol{v}\|^-$ and $\|\boldsymbol{v}\|^0$ for the sets of indices i such that $\boldsymbol{v}(i) > 0, \boldsymbol{v}(i) < 0$ and $\boldsymbol{v}(i) = 0$, respectively. We denote by $\|\boldsymbol{v}\|_\infty$ the *infinite norm* $\max_i |\boldsymbol{v}(i)|$. Given a finite set $\boldsymbol{V}$ of vectors, we introduce $\|\boldsymbol{V}\|_\infty = \max_{\boldsymbol{v} \in \boldsymbol{V}} \|\boldsymbol{v}\|_\infty$. A *word* is a finite sequence $\sigma = \boldsymbol{v}_1 \cdots \boldsymbol{v}_n$ of vectors in $\mathbb{Z}^d$. We let $|\sigma|$ denote the *length* n of the word σ. The *displacement* of σ is the sum $\sum_{j=1}^n \boldsymbol{v}_j$, denoted by $\Delta(\sigma)$.

We now recall the main concepts of vector addition systems (VAS). Consider a *dimension* $d \in \mathbb{N}$, with $d > 0$. A *configuration* is a vector $\boldsymbol{c} \in \mathbb{N}^d$, and an *action* is a vector $\boldsymbol{a} \in \mathbb{Z}^d$. Informally, a vector addition system moves from one configuration to the next by adding an action. This operational semantics is formalized by the labeled transition relation $\rightarrow \subseteq \mathbb{N}^d \times \mathbb{Z}^d \times \mathbb{N}^d$ defined by $\boldsymbol{c} \xrightarrow{\boldsymbol{a}} \boldsymbol{c}'$ if $\boldsymbol{c}' = \boldsymbol{c} + \boldsymbol{a}$. In particular, notice that an action $\boldsymbol{a}$ is enabled in a configuration $\boldsymbol{c}$ if, and only if, $\boldsymbol{c} + \boldsymbol{a} \geq \boldsymbol{0}$. A *run* is a finite, alternating sequence $(\boldsymbol{c}_0, \boldsymbol{a}_1, \boldsymbol{c}_1, \ldots, \boldsymbol{a}_n, \boldsymbol{c}_n)$ of configurations and actions, satisfying $\boldsymbol{c}_{i-1} \xrightarrow{\boldsymbol{a}_i} \boldsymbol{c}_i$ for all i. We write $\boldsymbol{c}_0 \xrightarrow{\boldsymbol{a}_1 \cdots \boldsymbol{a}_n} \boldsymbol{c}_n$ when the intermediate configurations are not important. The word $\boldsymbol{a}_1 \cdots \boldsymbol{a}_n$ is called the *label* of the run. A *trace* from a configuration $\boldsymbol{c}$ is the label of some run that starts with $\boldsymbol{c}$. Given an *initial configuration* $\boldsymbol{c}_{\text{init}} \in \mathbb{N}^d$, we let $\mathcal{T}(\boldsymbol{c}_{\text{init}})$ denote the set of all traces from $\boldsymbol{c}_{\text{init}}$.

A *vector addition system* is a pair $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ where $\boldsymbol{A}$ is a finite subset of $\mathbb{Z}^d$ and $\boldsymbol{c}_{\text{init}} \in \mathbb{N}^d$ is an initial configuration. Its operational semantics is obtained by restricting the labeled transition relation $\rightarrow$ to actions in $\boldsymbol{A}$. Accordingly, a *trace* of a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ is a trace from $\boldsymbol{c}_{\text{init}}$ that is contained in $\boldsymbol{A}^*$. The set of all traces of $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$, written $\mathcal{T}(\boldsymbol{A}, \boldsymbol{c}_{\text{init}}) = \mathcal{T}(\boldsymbol{c}_{\text{init}}) \cap \boldsymbol{A}^*$, is called the *trace language* of $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$.

In this paper, we consider verification properties that can be checked through witnesses that are traces satisfying some pumping conditions. These are called self-covering sequences, and defined as follows.

Definition 2.1. *A self-covering sequence for a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ is a non-empty sequence $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ of words such that $u_1 \sigma_1 \cdots u_k \sigma_k$ is a trace and $\|\Delta(\sigma_h)\|^- \subseteq \bigcup_{j=1}^{h-1} \|\Delta(\sigma_j)\|^+$ for all $h \in \{1, \ldots, k\}$.*

The words $\sigma_1, \ldots, \sigma_k$ are called *pumping segments*, k is the *number of pumping segments*, and $|u_1| + |\sigma_1| + \cdots + |u_k| + |\sigma_k|$ is the *size* of the self-covering sequence. If $k = 1$ in the above definition and $\|\Delta(\sigma_1)\|^+ \neq \emptyset$, we get the standard self-covering sequences, which are known to witness unboundedness of VAS [5]. The next lemma states a property of self-covering sequences that explains the name given to the words $\sigma_1, \ldots, \sigma_k$.

Lemma 2.2. *A sequence $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ of words is self-covering for a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ if, and only if, $u_1 \sigma_1 \ldots u_k \sigma_k$ is a trace and for every $n \in \mathbb{N}$, there exist $n_1, \ldots, n_k \geq n$ such that $u_1 \sigma_1^{n_1} \cdots u_k \sigma_k^{n_k}$ is a trace.*

3   A Relational Logic to Express Properties of Traces

In this section, we introduce a logic that can express properties of VAS such as unboundedness, place unboundedness, and non-regularity (see Section 4 for examples). The logic has terms t and formulas ϕ of the following syntax:

$$t ::= z\boldsymbol{\delta}_j(i) \mid t + t, \quad z \in \mathbb{Z}, j \geq 1, 1 \leq i \leq d$$
$$\phi ::= t \geq n \mid \phi \vee \phi \mid \phi \wedge \phi, \quad n \in \mathbb{N}$$

In the above syntax, $\boldsymbol{\delta}_j$ are variables that have to be interpreted. The norm $\|t\|_1$ of a term t is defined inductively as follows: $\|z\boldsymbol{\delta}_j(i)\|_1 = |z|$, $\|t_1 + t_2\|_1 = \|t_1\|_1 + \|t_2\|_1$. The norm $\|\phi\|_1$ of a formula ϕ is defined by $\|t \geq n\|_1 = \|t\|_1 + n$, $\|\phi_1 \vee \phi_2\|_1 = \|\phi_1 \wedge \phi_2\|_1 = \|\phi_1\|_1 + \|\phi_2\|_1$.

Definition 3.1. *A self-covering sequence $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ satisfies a formula ϕ if ϕ is true according to the usual laws of arithmetic when $\boldsymbol{\delta}_j$ is set to $\Delta(\sigma_j)$ for $j \leq k$ and $\boldsymbol{\delta}_j$ is set to $\boldsymbol{0}$ for $j > k$.*

A VAS satisfies a formula ϕ if it admits a self-covering sequence satisfying ϕ. The *model-checking* problem for this logic asks whether a given VAS satisfies a given formula.

Remark 3.2. The satisfaction of the formula does not depend on the words $u_1, \ldots, u_k$. However, without these words, the reachability problem for vector addition systems can be easily reduced to the model-checking problem for the logic. Recall that the reachability problem consists in deciding if a given configuration is the last configuration of a run starting from the initial one. This problem is known to be decidable[10, 6] but no complexity upper-bound is known. An adaptation of the proof of [1, Theorem 3] shows that the reachability problem for VAS can be reduced to the model-checking problem for our logic by additionally requiring that $u_1, \ldots, u_k$ are empty words. □

The model-checking problem for our logic can be solved by constructing the Karp & Miller coverability graph [5]. However, the size of the coverability graph can be Ackermann in the size of the VAS. We will show in Sections 5 up to 7 that this problem can be solved in exponential space. Before that, let us present some applications of our logic.

4   Examples and Short Extensions

In this section, we show that classical problems can be reduced to the model-checking problem for our logic. We prove that unboundedness, place unboundedness and non-regularity can be directly encoded with formulas. We also provide

short extensions of the logic based on simple encodings that can express recurrence and coverability. All these problems are recalled in this section.

We first present problems that can be directly reduced to the model-checking problem for our logic. Recall that a configuration c is *reachable* if there is a run from the initial configuration to c. The set of reachable configurations is called the *reachability set*. A vector addition system is *bounded* if its reachability set is finite. The boundedness problem was proved to be decidable by Karp and Miller in [5]. The decidability comes from a characterization of unbounded vector addition systems; a vector addition system is unbounded if, and only if, there exists a self-covering sequence (u_1, σ_1) such that $\|\Delta(\sigma_1)\|^+ \neq \emptyset$. Karp and Miller provided a way for deciding this property based on the computation of a tree (the Karp & Miller coverability tree). The complexity of this algorithm is non-primitive recursive [11]. Lipton proved in [9] that the boundedness problem requires exponential space. In [13], Rackoff provided an exponential space upper bound based on a doubly-exponential bound on self-covering sequences witnessing unboundedness. We observe that a vector addition system is unbounded if, and only if, it satisfies the following formula:

$$\bigvee_{i=1}^{d} \boldsymbol{\delta}_1(i) \geq 1$$

The boundedness problem was generalized by introducing variants like the place boundedness problem that asks which components (also called places for Petri nets) are unbounded. The place boundedness problem requires exponential space. The proof is by a simple reduction from the boundedness problem. Whereas the place boundedness problem was considered in different papers, no upper bound of complexity was published until recently in [3]. In that paper, Demri introduced a more general problem, useful for reducing different problems, called the simultaneous unboundedness problem. A vector addition system is *simultaneously unbounded* on a set $I \subseteq \{1, \ldots, d\}$ of indexes, if, for every bound $b \in \mathbb{N}$, there exists a reachable configuration c such that $c(i) \geq b$ for every $i \in I$. Demri proved that a vector addition system is simultaneously unbounded on I if, and only if, it satisfies the following formula:

$$\bigwedge_{i \in I} \bigvee_{j=1}^{d} \boldsymbol{\delta}_j(i) \geq 1$$

A vector addition system is called *regular* when its trace language is regular. In [16], Valk and Vidal-Naquet provided a characterization of non-regularity for vector addition systems. Since the characterization is based on the Karp & Miller coverability graph [5], the Valk and Vidal-Naquet algorithm is non-primitive recursive. In [1], Atig and Habermehl observed that the regularity problem cannot be expressed in their fragment of Yen's path logic that is decidable in exponential space, and left the complexity open. Based on the simultaneous unboundedness approach, Demri proved in [3] that the regularity problem is decidable in exponential space. This upper bound is obtained by observing that the trace language

of a VAS is non-regular if, and only if, the VAS satisfies the following formula:

$$\bigvee_{i=1}^{d} -\boldsymbol{\delta}_{d+1}(i) \geq 1$$

Till now, we proved that some classical problems can be reduced to the model-checking problem for our logic. For other problems, we need short extensions that require simple encodings. In the remainder of this section, we show the kind of extensions that can be useful for deciding recurrence and coverability problems.

A set of actions $\boldsymbol{T}$ of a vector addition system is said to be *recurrent* if there exists a self-covering sequence (u_1, σ_1) such that $\boldsymbol{T}$ is the set of actions occurring in σ_1. The verification of LTL properties and some other properties like promptness detection (see, e.g., [1, 15]) can be reduced to the recurrence problem. The latter problem can be reduced to the model-checking problem for our logic by introducing extra components, one for each action, counting the number of times an action is executed. Let us consider a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ and a subset $\boldsymbol{T} \subseteq \boldsymbol{A}$. We assume that $\boldsymbol{A} = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$. Recall that $\boldsymbol{e}_\ell$ is the unit vector defined by $\boldsymbol{e}_\ell(\ell) = 1$ and $\boldsymbol{e}_\ell(i) = 0$ if $i \neq \ell$. We introduce the VAS $\langle \boldsymbol{A}', \boldsymbol{c}'_{\text{init}} \rangle$ of dimension $d + n$ defined by $\boldsymbol{A}' = \{(\boldsymbol{a}_\ell, \boldsymbol{e}_\ell) \mid 1 \leq \ell \leq n\}$ and $\boldsymbol{c}'_{\text{init}} = (\boldsymbol{c}_{\text{init}}, \boldsymbol{0})$. Observe that $\boldsymbol{T}$ is recurrent for the VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ if, and only if, $\langle \boldsymbol{A}', \boldsymbol{c}'_{\text{init}} \rangle$ satisfies the following formula:

$$\bigwedge_{j | \boldsymbol{a}_j \in \boldsymbol{T}} \boldsymbol{\delta}_1(d+j) \geq 1 \quad \wedge \quad \bigwedge_{j | \boldsymbol{a}_j \notin \boldsymbol{T}} -\boldsymbol{\delta}_1(d+j) \geq 0$$

The same transformation provides a simple way for encoding more complex relations between numbers of occurrences in different pumping segments of self-covering sequences. For instance, the strong promptness detection (see, e.g., [1]) can be encoded with the previous formula by replacing $\boldsymbol{\delta}_1$ by $\boldsymbol{\delta}_d$.

One can also check coverability properties with the help of an additional component. Recall that a configuration $\boldsymbol{c} \in \mathbb{N}^d$ is *coverable* if there exists a reachable configuration larger than or equal to $\boldsymbol{c}$, i.e., a reachable configuration in $\boldsymbol{c} + \mathbb{N}^d$. The coverability problem asks whether a given configuration is coverable in a given VAS. Lipton derived an exponential space lower bound in [9] and Rackoff provided an exponential space upper bound in [13]. The coverability problem can be reduced to the place boundedness problem as follows. Given a vector addition system $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ and a configuration $\boldsymbol{c}$, we consider the vector addition system $\langle \boldsymbol{A}', \boldsymbol{c}'_{\text{init}} \rangle$ defined by $\boldsymbol{A}' = (\boldsymbol{A} \times \{0\}) \cup \{(-\boldsymbol{c}, 2), (\boldsymbol{c}, -1)\}$ and $\boldsymbol{c}'_{\text{init}} = (\boldsymbol{c}_{\text{init}}, 0)$. Just observe that $\boldsymbol{c}$ is coverable in $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ if, and only if, the last component of the VAS $\langle \boldsymbol{A}', \boldsymbol{c}'_{\text{init}} \rangle$ is unbounded. Therefore, the coverability problem can be reduced to the model-checking problem for our logic. With a similar transformation, we can encode more complex properties that require multiple coverings along the pumping segments of a self-covering sequence.

5 Small Model Property

In this section, we show that if there is a self-covering sequence satisfying a formula, there is one whose length is bounded in terms of the sizes of the VAS and the formula. As a consequence, we get ExpSpace-completeness for the model-checking problem for our logic.

The bound we give for the size of satisfying self-covering sequences depends in a specific way on how conjunctions are distributed in a formula. We define below two measures of formulas that will be used in our bound.

Definition 5.1. *For a formula ϕ, the* conjunction rank $r(\phi)$ *is defined inductively as follows: $r(t \geq n) = 1$, $r(\phi_1 \vee \phi_2) = \max\{r(\phi_1), r(\phi_2)\}$ and $r(\phi_1 \wedge \phi_2) = r(\phi_1) + r(\phi_2)$. By $k(\phi)$ we denote the maximal j such that $\boldsymbol{\delta}_j$ occurs in ϕ.*

Intuitively, $r(\phi)$ is a bound on the number of terms that need to be satisfied simultaneously to satisfy ϕ.

Theorem 5.2. *If there is a self-covering sequence in $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ satisfying ϕ, there is one of size at most $(\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c^{(d \cdot k(\phi))^3}}$ where c is a constant.*

The proof is in two parts. The first part is bounding the lengths of $u_1, \ldots, u_k$ that occur in between the pumping segments $\sigma_1, \ldots, \sigma_k$. We will make use of the following result, which is an easy consequence of some proofs given in [13].

Lemma 5.3. *Suppose that $\boldsymbol{c}_{init} \xrightarrow{\sigma} \boldsymbol{c}_1$ and $\boldsymbol{c}_1 \geq \boldsymbol{c}$. Then there is a sub-word σ' of σ such that $\boldsymbol{c}_{init} \xrightarrow{\sigma'} \boldsymbol{c}_1'$, $\boldsymbol{c}_1' \geq \boldsymbol{c}$ and $|\sigma'| \leq (\|\boldsymbol{A}\|_\infty + \|\boldsymbol{c}\|_\infty)^{(d+1)!}$.*

Proof. Follows easily from a close observation of [13, Proof of Lemma 3.4]. □

Lemma 5.4. *Consider a run $\boldsymbol{c}_{init} \xrightarrow{u_1} \boldsymbol{c}_1 \xrightarrow{\sigma_1} \boldsymbol{c}_1' \rightarrow \cdots \xrightarrow{u_k} \boldsymbol{c}_k \xrightarrow{\sigma_k} \boldsymbol{c}_k'$ of $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$, with $|\sigma_1| + \cdots + |\sigma_k| \leq l$. Then there are words $u_1', \ldots, u_k'$ such that $u_1' \sigma_1 \cdots u_k' \sigma_k$ is a trace and $|u_1'| + \cdots + |u_k'| \leq (2l\|\boldsymbol{A}\|_\infty)^{((d+1)k+1)!}$.*

Proof (Sketch). For any word σ, let $\boldsymbol{c}_\sigma$ be the unique minimal configuration that enables σ. Since $\boldsymbol{c}_j \geq \boldsymbol{c}_{\sigma_j}$ for all j, $1 \leq j \leq k$, $\boldsymbol{c}_{\sigma_j}$ are all coverable from $\boldsymbol{c}_{init}$. Let $\boldsymbol{c}_{init}^k$ be the vector obtained by adjoining k copies of $\boldsymbol{c}_{init}$ and let $\boldsymbol{c}''$ be the vector obtained by adjoining $\boldsymbol{c}_{\sigma_1}, \ldots, \boldsymbol{c}_{\sigma_k}$. We can now think of a suitably defined new VAS where $\boldsymbol{c}''$ is coverable from the initial configuration $\boldsymbol{c}_{init}^k$. From Lemma 5.3, we infer that there is a sub-word of the original covering sequence that also covers $\boldsymbol{c}''$, whose length is bounded. From this short covering sequence, we extract words $u_1', \ldots, u_k'$ of the original VAS satisfying the length requirements. □

Now it is enough to bound the length of the pumping segments. Suppose $\boldsymbol{c}_{init} \xrightarrow{u_1} \boldsymbol{c}_1 \xrightarrow{\sigma_1} \boldsymbol{c}_1' \rightarrow \cdots \xrightarrow{u_k} \boldsymbol{c}_k \xrightarrow{\sigma_k} \boldsymbol{c}_k'$. Indices in $\|\sigma_1\|^+$ can potentially reach arbitrarily high values (by repeating σ_1 many times). We want to momentarily forget the exact value of these indices and emphasize that they can be as large as needed. This is done by allowing values to be ω.

Definition 5.5. *Let $\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$. Let $\omega \geq n$ and $\omega - n = \omega + n = \omega$ for all $n \in \mathbb{N}$. An extended configuration is a vector $\boldsymbol{x} \in \mathbb{N}_\omega^d$. The labeled transition relation $\to$ is extended to $\to \subseteq \mathbb{N}_\omega^d \times \mathbb{Z}^d \times \mathbb{N}_\omega^d$ defined by $\boldsymbol{x} \xrightarrow{a} \boldsymbol{x}'$ if $\boldsymbol{x}' = \boldsymbol{x} + \boldsymbol{a}$. We denote by $\|\boldsymbol{x}\|^\omega$ the set of indices i such that $\boldsymbol{x}(i) = \omega$.*

Let $\boldsymbol{x}_1$ be the extended configuration that is the same as $\boldsymbol{c}_1$ except in indices that are increased by σ_1, where $\boldsymbol{x}_1$ has ω. That is, let $\boldsymbol{x}_1(i) = \omega$ for $i \in \|\Delta(\sigma_1)\|^+$ and $\boldsymbol{x}_1(i) = \boldsymbol{c}_1'(i) = \boldsymbol{c}_1(i)$ for $i \in \|\Delta(\sigma_1)\|^0$ ($\|\Delta(\sigma_1)\|^- = \emptyset$). Similarly, let $\boldsymbol{x}_2(i) = \omega$ for $i \in \|\sigma_1\|^+ \cup \|\sigma_2\|^+$ and $\boldsymbol{x}_2(i) = \boldsymbol{c}_2'(i) = \boldsymbol{c}_2(i)$ for $i \in \|\Delta(\sigma_2)\|^0 \setminus \|\sigma_1\|^+$ ($\|\Delta(\sigma_2)\|^- \subseteq \|\sigma_1\|^+$). The extended configurations $\boldsymbol{x}_3, \ldots, \boldsymbol{x}_k$ are similar.

We have $\boldsymbol{x}_j \xrightarrow{\sigma_j} \boldsymbol{x}_j$ for all j, $1 \leq j \leq k$, which can be thought of as $\boldsymbol{x} \xrightarrow{\sigma} \boldsymbol{x}$ in a suitably defined (kd)-dimensional VAS. Hence, σ is a cycle on $\boldsymbol{x}$ in this new VAS. Note that $\Delta(\sigma)$ is not necessarily $\boldsymbol{0}$, since $\boldsymbol{x}$ may have some omega components. The fact that $\sigma_1, \ldots, \sigma_k$ are pumping segments satisfying ϕ can be encoded into a linear system of the form $\boldsymbol{Z}\Delta(\sigma) \geq \boldsymbol{n}$. We prove in the next section that if there are cycles satisfying such a condition, there will be similar cycles of bounded length. From such a short cycle, we can extract words $\sigma_1', \ldots, \sigma_k'$ of the original VAS meeting the length requirements of Theorem 5.2.

6 Short Cycles via Reversibility Domains

In this section, we show that for every cycle $\boldsymbol{x} \xrightarrow{\sigma} \boldsymbol{x}$ satisfying a linear system, there exists a similar short cycle $\boldsymbol{x} \xrightarrow{\sigma'} \boldsymbol{x}$. The proof is based on the following two theorems providing bounds related to reversible words. These results are proved in [7]. Given an implicit VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$, a word $u \in \boldsymbol{A}^*$ is said to be *reversible* on an extended configuration $\boldsymbol{c}$ if there exists a word $v \in \boldsymbol{A}^*$ such that $\boldsymbol{c} \xrightarrow{uv} \boldsymbol{c}$ and such that $\Delta(uv) = \boldsymbol{0}$. The *domain of reversibility* of an action $\boldsymbol{a} \in \boldsymbol{A}$ is the set of extended configurations $\boldsymbol{c}$ on which $\boldsymbol{a}$ is reversible.

Theorem 6.1 ([7, Theorem 10.1]). *Let $u \in \boldsymbol{A}^*$ be a reversible word on an extended configuration $\boldsymbol{c}$. There exists $u' \in \boldsymbol{A}^*$ reversible on $\boldsymbol{c}$ such that $\Delta(u) = \Delta(u')$ and $|u'| \leq 17d^2 x^{15d^{d+2}}$, where $x = (1 + \|\boldsymbol{A}\|_\infty)(1 + \|\boldsymbol{c}\|_\infty + \|\Delta(u)\|_\infty)$.*

Theorem 6.2 ([7, Theorem 11.1]). *For every extended configuration $\boldsymbol{c}$ in the domain of reversibility of an action $\boldsymbol{a} \in \boldsymbol{A}$, there exists a configuration $\boldsymbol{c}' \leq \boldsymbol{c}$ in the domain of reversibility of $\boldsymbol{a}$ such that $\|\boldsymbol{c}'\|_\infty \leq (102d^2\|\boldsymbol{A}\|_\infty^2)^{(15d^{d+2})^{d+2}}$.*

To show the existence of such short cycles, we need to introduce some notations and a technical result regarding minimal solutions of linear diophantine systems. For an integer vector $\boldsymbol{v}$, let $\|\boldsymbol{v}\|_1$ denote the sum $\sum_i |\boldsymbol{v}(i)|$. For a finite set of vectors $\boldsymbol{V}$, $\|\boldsymbol{V}\|_1$ denotes $\max_{\boldsymbol{v} \in \boldsymbol{V}}\{\|\boldsymbol{v}\|_1\}$. For an integer matrix $\boldsymbol{Z}$, let $\|\boldsymbol{Z}\|_{1,\infty}$ denote $\max_i\{\sum_j |\boldsymbol{Z}(i,j)|\}$. For $z \in \mathbb{Z}$, let $z\boldsymbol{v}$ denote the vector such that $(z\boldsymbol{v})(i) = z \cdot \boldsymbol{v}(i)$ for all i. Let $\mathbb{N}\boldsymbol{v}$ denote the set of vectors $\{n\boldsymbol{v} \mid n \in \mathbb{N}\}$. For two sets of vectors $\boldsymbol{V}_1, \boldsymbol{V}_2$ of the same dimension, let $\boldsymbol{V}_1 + \boldsymbol{V}_2$ denote the set of vectors $\{\boldsymbol{v}_1 + \boldsymbol{v}_2 \mid \boldsymbol{v}_1 \in \boldsymbol{V}_1, \boldsymbol{v}_2 \in \boldsymbol{V}_2\}$.

Based on [12], one can easily derive the following lemma.

Lemma 6.3. *Let $\boldsymbol{Z}$ be a $r \times d$ integer matrix and let $\boldsymbol{b} \in \mathbb{Z}^r$ be a vector. The set of all integer vectors $\boldsymbol{\rho}$ such that $\boldsymbol{Z}\boldsymbol{\rho} \geq \boldsymbol{b}$ is a finite union of sets of the form $\boldsymbol{p}_0 + \mathbb{N}\boldsymbol{p}_1 + \cdots + \mathbb{N}\boldsymbol{p}_m$, where $m \in \mathbb{N}$ and $\boldsymbol{p}_0, \boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ are integer vectors such that $\|\boldsymbol{p}_0\|_1, \|\boldsymbol{p}_1\|_1, \ldots, \|\boldsymbol{p}_m\|_1 \leq (2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{b}\|_\infty)^r$.*

Now we are ready to prove the existence of short cycles.

Lemma 6.4. *Let $\boldsymbol{A} \subseteq \mathbb{Z}^d$ be a finite set and $\boldsymbol{x} \in \mathbb{N}_\omega^d$ be an extended configuration. Suppose there is a word $\sigma \in \boldsymbol{A}^*$ such that $\boldsymbol{x} \xrightarrow{\sigma} \boldsymbol{x}$ and $\boldsymbol{Z}\Delta(\sigma) \geq \boldsymbol{n}$, where $\boldsymbol{Z} \in \mathbb{Z}^{r \times d}$ is an integer matrix with r rows, d columns and $\boldsymbol{n} \in \mathbb{N}^r$ is a vector of natural numbers. Then there is a word $\sigma' \in \boldsymbol{A}^*$ such that $\boldsymbol{x} \xrightarrow{\sigma'} \boldsymbol{x}$, $\boldsymbol{Z}\Delta(\sigma') \geq \boldsymbol{n}$ and $|\sigma'| \leq (\|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty)^{rc_2^{d^3}}$ for some constant c_2.*

Proof. Since $\boldsymbol{x} \xrightarrow{\sigma} \boldsymbol{x}$, $\Delta(\sigma)(i) = 0$ for all $i \notin \|\boldsymbol{x}\|^\omega$. We can encode these conditions as additional inequalities in $\boldsymbol{Z}\Delta(\sigma) \geq \boldsymbol{n}$, by adding at most $2d$ rows to $\boldsymbol{Z}$ and $\boldsymbol{n}$. Let $\boldsymbol{Z}'\Delta(\sigma) \geq \boldsymbol{n}'$ be the resulting system. By Lemma 6.3, the set of all vectors $\boldsymbol{\rho} \in \mathbb{Z}^d$ satisfying $\boldsymbol{Z}'\boldsymbol{\rho} \geq \boldsymbol{n}'$ is a finite union of sets of the form $\boldsymbol{p}_0 + \mathbb{N}\boldsymbol{p}_1 + \cdots + \mathbb{N}\boldsymbol{p}_m$, where $m \in \mathbb{N}$ and $\boldsymbol{p}_0, \boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ are integer vectors such that $\|\boldsymbol{p}_0\|_1, \|\boldsymbol{p}_1\|_1, \ldots, \|\boldsymbol{p}_m\|_1 \leq (2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{n}'\|_\infty)^{r+2d}$. Since $\boldsymbol{Z}'\boldsymbol{p}_0 \geq \boldsymbol{n}'$ and $\boldsymbol{n}'$ is a vector of natural numbers, we have $\boldsymbol{Z}'(i\boldsymbol{p}_0) \geq \boldsymbol{n}'$ for all $i \geq 1$. Hence, we can assume without loss of generality that the sets are of the form $\boldsymbol{p}_0 + \mathbb{N}\boldsymbol{p}_0 + \mathbb{N}\boldsymbol{p}_1 + \cdots + \mathbb{N}\boldsymbol{p}_m$. Since $\boldsymbol{Z}'\boldsymbol{p}_0 \geq \boldsymbol{n}'$, $\boldsymbol{p}_0(i) = 0$ for $i \notin \|\boldsymbol{x}\|^\omega$. Since $\boldsymbol{Z}'(\boldsymbol{p}_0 + \boldsymbol{p}_j) \geq \boldsymbol{n}'$ for all $j \in \{1, \ldots, m\}$, $(\boldsymbol{p}_0 + \boldsymbol{p}_j)(i) = 0$ for $i \notin \|\boldsymbol{x}\|^\omega$. Hence, $\boldsymbol{p}_j(i) = 0$ for $i \notin \|\boldsymbol{x}\|^\omega$ and $j \in \{1, \ldots, m\}$. In words, this means that vectors $\boldsymbol{p}_0, \boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ have value 0 in indices that are not ω in $\boldsymbol{x}$.

Suppose $\Delta(\sigma) = \boldsymbol{p}_0 + i_0\boldsymbol{p}_0 + \cdots + i_m\boldsymbol{p}_m$. Let $\widetilde{\boldsymbol{A}} = \boldsymbol{A} \cup \{-\boldsymbol{p}_0, \ldots, -\boldsymbol{p}_m\}$. We have $\boldsymbol{x} \xrightarrow{-\boldsymbol{p}_0} \boldsymbol{x} \xrightarrow{(-\boldsymbol{p}_0)^{i_0} \cdots (-\boldsymbol{p}_m)^{i_m}\sigma} \boldsymbol{x}$, written as $\boldsymbol{x} \xrightarrow{-\boldsymbol{p}_0} \boldsymbol{x} \xrightarrow{u} \boldsymbol{x}$ for simplicity. By our choice of $i_0, \ldots, i_m$, we get $\Delta(u) = \boldsymbol{p}_0$. This means the action $-\boldsymbol{p}_0$ is *reversible* on the extended configuration $\boldsymbol{x}$. Hence, by Theorem 6.2, there exists a configuration $\boldsymbol{c}' \leq \boldsymbol{x}$ such that $-\boldsymbol{p}_0$ is reversible on $\boldsymbol{c}'$ and $\|\boldsymbol{c}'\|_\infty \leq (102d^2\tilde{a}^2)^{(15d^{d+2})^{d+2}}$, where $\tilde{a} = \|\widetilde{\boldsymbol{A}}\|_\infty$. Now we have $\boldsymbol{c}' \xrightarrow{-\boldsymbol{p}_0} \boldsymbol{c}'' \xrightarrow{u'} \boldsymbol{c}'$, so $\Delta(u') = \boldsymbol{p}_0$. The word u' is reversible on the configuration $\boldsymbol{c}''$. By Theorem 6.1, there exists another word u'' reversible on $\boldsymbol{c}''$ such that $\Delta(u'') = \Delta(u') = \boldsymbol{p}_0$ and $|u''| \leq 17d^2x^{15d^{d+2}}$, where $x = (1 + 2\|\widetilde{\boldsymbol{A}}\|_\infty)(1 + \|\boldsymbol{c}''\|_\infty + \|\Delta(u')\|_\infty)$.

Let σ' be the word obtained from u'' by retaining only the actions in $\boldsymbol{A}$. We get $\Delta(u'') = \Delta(\sigma') - i_0'\boldsymbol{p}_0 - \cdots - i_m'\boldsymbol{p}_m$ by introducing i_j', the number of times $-\boldsymbol{p}_j$ occurs in u''. Hence $\Delta(\sigma') = \boldsymbol{p}_0 + i_0'\boldsymbol{p}_0 + \cdots + i_m'\boldsymbol{p}_m$, since $\Delta(u'') = \boldsymbol{p}_0$.

It follows that $\boldsymbol{Z}'\Delta(\sigma') \geq \boldsymbol{n}'$ and so $\boldsymbol{Z}\Delta(\sigma') \geq \boldsymbol{n}$. Recall that $\boldsymbol{c}' \leq \boldsymbol{c} \leq \boldsymbol{x}$ and that $\boldsymbol{c}' \xrightarrow{-\boldsymbol{p}_0} \boldsymbol{c}'' \xrightarrow{u''} \boldsymbol{c}'$. Since σ' is obtained from u'' by removing some actions in $\widetilde{\boldsymbol{A}} \setminus \boldsymbol{A}$ and since those actions have value 0 in indices where $\boldsymbol{x}$ is not ω, we infer that $\boldsymbol{x} \xrightarrow{-\boldsymbol{p}_0} \boldsymbol{x} \xrightarrow{\sigma'} \boldsymbol{x}$. It remains to bound the length of σ' to conclude the proof. We have $x = (1 + 2\|\widetilde{\boldsymbol{A}}\|_\infty)(1 + \|\boldsymbol{c}''\|_\infty + \|\Delta u'\|_\infty)$ and $|\sigma'| \leq |u''| \leq 17d^2x^{15d^{d+2}}$. After some simplifications, it can be inferred that $|\sigma'| \leq (\|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty)^{rc_2^{d^3}}$ for a suitably chosen constant c_2. The

9

simplification involves calculations that are a bit tedious and can be found in the appendix. □

In Lemma 6.4 above, $\boldsymbol{n}$ is a vector of natural numbers in the linear system $\boldsymbol{Z}\Delta(\sigma) \geq \boldsymbol{n}$. It is unlikely that a similar result about short cycles can be proved when $\boldsymbol{n}$ is an integer vector, since that would imply short witnesses for reachability, as shown by the following remark.

Remark 6.5. Let $\boldsymbol{c}_{\text{init}} \xrightarrow{u} \boldsymbol{c}$ be a run in a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$. We associate to every action $\boldsymbol{a}$ the action $\tilde{\boldsymbol{a}} = (\boldsymbol{a}, 0)$ with an extra component equal to zero. We also introduce the set $\tilde{\boldsymbol{A}} = \{\tilde{\boldsymbol{a}} \mid \boldsymbol{a} \in \boldsymbol{A}\} \cup \{(\boldsymbol{c}_{\text{init}}, 2), (-\boldsymbol{c}, 3)\}$. From the word $u = \boldsymbol{a}_1 \dots \boldsymbol{a}_k$ we get the word $\tilde{u} = \tilde{\boldsymbol{a}}_1 \dots \tilde{\boldsymbol{a}}_k$. Now observe that $\sigma = (\boldsymbol{c}_{\text{init}}, 2)\tilde{u}(-\boldsymbol{c}, 3)$ and $\boldsymbol{x} = (\boldsymbol{0}, \omega)$ satisfies $\boldsymbol{x} \xrightarrow{\sigma} \boldsymbol{x}$ and $\Delta(\sigma)(d+1) = 5$, which can be encoded by two inequalities provided that we allow comparisons with negative integers (as we only permit $\geq$). Moreover from any word $\sigma' \in \tilde{\boldsymbol{A}}^*$ such that $\boldsymbol{x} \xrightarrow{\sigma'} \boldsymbol{x}$ and $\Delta(\sigma')(d+1) = 5$ we derive a word $u' \in \boldsymbol{A}^*$ such that $|u'| = |\sigma'| - 2$ and $\boldsymbol{c}_{\text{init}} \xrightarrow{u'} \boldsymbol{c}$. In fact, we observe that u' contains one occurrence of $(\boldsymbol{c}_{\text{init}}, 2)$ and one occurrence of $(-\boldsymbol{c}, 3)$. By removing these occurrences from σ', we get u'. □

7 Small Pumping Segments through Short Cycles

In this section, we use the result of the previous section to prove Theorem 5.2. We first provide a bound on the pumping segments.

Lemma 7.1. *Suppose there is a self-covering sequence $(u_1, \sigma_1, \dots, u_k, \sigma_k)$ satisfying ϕ. Then there is a self-covering sequence $(u_1', \sigma_1', \dots, u_k', \sigma_k')$ satisfying ϕ such that $|\sigma_1'| + \dots + |\sigma_k'| \leq (\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c_1^{(d \cdot k(\phi))^3}}$ where c_1 is a constant.*

Proof (Sketch). A self-covering sequence $(u_1, \sigma_1, \dots, u_k, \sigma_k)$ satisfies a formula $t \geq n$ if, and only if, $\boldsymbol{z} \odot (\Delta(\sigma_1), \dots, \Delta(\sigma_k)) \geq n$, where $\boldsymbol{z} \in \mathbb{Z}^{d \cdot k}$ is an integer vector that only depends on t, $\odot$ is the usual dot product. The conditions $\|\Delta(\sigma_j)\|^- \subseteq \cup_{1 \leq j' < j} \|\Delta(\sigma_{j'})\|^+$ can also be expressed as a set of inequalities of the previous form. By suitably defining a (kd)-dimensional VAS, we can think of a word σ whose displacement is $(\Delta(\sigma_1), \dots, \Delta(\sigma_k))$. The combination of all the satisfied terms of ϕ and the condition for self-covering sequences gives rise to a linear system $\boldsymbol{Z}\Delta(\sigma) \geq \boldsymbol{n}$, where $\boldsymbol{Z}$ is an integer matrix and $\boldsymbol{n}$ is a vector of natural numbers.

Using the result of the previous section, we find a short cycle labeled by σ' whose displacement also satisfies $\boldsymbol{Z}\Delta(\sigma') \geq \boldsymbol{n}$. From this short cycle, we can extract words of the original VAS which are pumping segments satisfying the length requirements of the lemma. □

We now have the necessary ingredients to prove our main result, Theorem 5.2. Assume that $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ admits a self-covering sequence $(u_1, \sigma_1, \dots, u_k, \sigma_k)$ satisfying ϕ. By Lemma 7.1, there exists a self-covering sequence $(u_1', \sigma_1', \dots, u_k', \sigma_k')$ satisfying ϕ such that $|\sigma_1'| + \dots + |\sigma_k'| \leq (\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c_1^{(k(\phi) \cdot d)^3}}$. We derive

from Lemma 5.4 that there exists a self-covering sequence $(u_1'', \sigma_1', \ldots, u_k'', \sigma_k')$ such that $|u_1''| + \cdots + |u_k''| \leq (2\|\boldsymbol{A}\|_\infty (\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c_1^{(k(\phi)\cdot d)^3}})^{((d+1)k(\phi)+1)!}$. Simplifying this, we get $|\sigma_1'| + \cdots + |\sigma_k'| + |u_1''| + \cdots + |u_k''| \leq (\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c^{(k(\phi)\cdot d)^3}}$ for a suitably chosen constant c, which concludes the proof of the theorem.

We now define the size of a VAS and a formula and state a complexity theoretic consequence of the small model property obtained above. The *size* of a VAS is the obvious one, where integers are encoded in binary. The *size* $|t|$ of a term t is defined inductively as follows: $|z\boldsymbol{\delta}_j(i)| = \log(|z| + 1)$ and $|t_1 + t_2| = 1 + |t_1| + |t_2|$. The *size* $|\phi|$ of a formula ϕ is defined by $|t \geq n| = |t| + 1 + \log(n+1)$, $|\phi_1 \vee \phi_2| = |\phi_1| + 1 + |\phi_2|$ and $|\phi_1 \wedge \phi_2| = |\phi_1| + 1 + |\phi_2|$.

Corollary 7.2. *Given a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ and a formula ϕ, the problem of checking whether there is a self-covering sequence satisfying ϕ is* ExpSpace-*complete.*

Proof. For the exponential space lower bound, we have seen in Section 4 that we can reduce the boundedness problem to checking a formula of our logic. Since the boundedness problem is ExpSpace-hard [9], checking whether a given formula is satisfied by a given VAS is ExpSpace-hard.

For the exponential space upper bound, a non-deterministic Turing machine can guess and verify the existence of a self-covering sequence of length at most $(\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c^{(d\cdot k(\phi))^3}}$. The Turing machine needs to maintain a counter to count (in binary) up to a maximum of $(\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c^{(d\cdot k(\phi))^3}}$ and store at most $2k$ intermediate configurations. The memory requirement is therefore $\mathcal{O}(r(\phi)c^{(d\cdot k(\phi))^3}(\log \|\boldsymbol{A}\|_\infty + \log \|\phi\|_1))$. It is easy to see that the size of the VAS is an upper bound on $\log \|\boldsymbol{A}\|_\infty$ and the size $|\phi|$ of the formula ϕ is an upper bound on $\log \|\phi\|_1$. Hence, the well-known Savitch's theorem then gives a deterministic Turing machine that works in exponential space. $\square$

8 Complexity of the Context-Freeness Problem for VAS

We have shown in the previous sections that the model-checking problem for our logic can be solved in exponential space. As an application, we now focus on the context-freeness problem for VAS, and characterize its complexity.

The context-freeness problem asks whether the trace language of a given VAS is context-free. This problem was shown to be decidable by Schwer in [14]. Since it is based on the coverability graph, the resulting algorithm's complexity is non-primitive recursive. Recently, we revisited the context-freeness problem for VAS, and gave a simpler proof of decidability [8]. Our approach is based on regular bounded languages having a non-context free intersection with the set of traces. In this section, we briefly recall this characterization. Then, we show how to express it by a formula in our logic, thereby providing an exponential space upper bound for the context-freeness problem.

A pair $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ of vectors in $\mathbb{Z}^d$ such that $\boldsymbol{v}_1 \geq \boldsymbol{0}$ and $\boldsymbol{v}_2 \not\geq \boldsymbol{0}$ is called a *matching pair*. For every matching pair $(\boldsymbol{v}_1, \boldsymbol{v}_2)$, there exists a maximal non-negative rational number $\lambda \geq 0$ such that $\boldsymbol{v}_1 + \lambda\boldsymbol{v}_2 \geq \boldsymbol{0}$. We call this rational

number the *ratio* of the matching pair $(\boldsymbol{v}_1, \boldsymbol{v}_2)$, and we denote it by $\mathsf{rat}(\boldsymbol{v}_1, \boldsymbol{v}_2)$. We define the *excess* of $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ as the vector $\mathsf{exc}(\boldsymbol{v}_1, \boldsymbol{v}_2) = \boldsymbol{v}_1 + \mathsf{rat}(\boldsymbol{v}_1, \boldsymbol{v}_2) \cdot \boldsymbol{v}_2$. Note that $\mathsf{exc}(\boldsymbol{v}_1, \boldsymbol{v}_2) \geq \boldsymbol{0}$.

A *matching scheme* is a tuple $(\sigma_1, \ldots, \sigma_k, U)$ where $\sigma_1, \ldots, \sigma_k$ are words in $(\mathbb{Z}^d)^*$ and U is a nested binary relation on $\{1, \ldots, k\}$ such that $(\Delta(\sigma_s), \Delta(\sigma_t))$ is a matching pair for every $(s, t) \in U$. Here, by *nested*, we mean that U satisfies the two following conditions:

$$(s, t) \in U \;\Rightarrow\; s \leq t \tag{1}$$

$$(r, t) \in U \,\wedge\, (s, u) \in U \;\Rightarrow\; \neg(r < s < t < u) \tag{2}$$

The *excess* of a matching scheme $(\sigma_1, \ldots, \sigma_k, U)$ is the vector $\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U) = \sum_{(s,t) \in U} \mathsf{exc}(\Delta(\sigma_s), \Delta(\sigma_t))$.

Definition 8.1. *A* witness of non-context-freeness *for a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ is a tuple $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$, where u_i, σ_i are words in $\boldsymbol{A}^*$ and $(\sigma_1, \ldots, \sigma_k, U)$ is a matching scheme, such that:*

1. *The word $u_1 \sigma_1 \cdots u_k \sigma_k$ is a trace of $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$,*
2. *It holds that $\Delta(\sigma_k) \not\geq \boldsymbol{0}$ and $\|\Delta(\sigma_k)\|^- \subseteq \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+$, and*
3. *For every $(s, t) \in U$ with $t < k$, there exists $(r, t) \in U$ such that $r \leq s$ and $\|\Delta(\sigma_t)\|^- \subseteq \|\Delta(\sigma_r)\|^+$.*

Theorem 8.2 ([8]). *The trace language of a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ is not context-free if, and only if, $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ admits a witness of non-context-freeness.*

Our objective is to express non-context-freeness by a formula in our relational trace logic. However, the conditions of Definition 8.1 cannot be translated, as is, in the logic. Firstly, the number k of pumping segments is not, a priori, bounded. Secondly, the sequence $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ need not be a self-covering sequence. Lastly, membership of a given index in the set $\|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+$ is not linear[1] in $\Delta(\sigma_1), \ldots, \Delta(\sigma_k)$ since it requires comparing ratios between components. To overcome this difficulty, we show that it is enough to look for witnesses of non-context-freeness satisfying additional, simplifying requirements.

Formally, a witness of non-context-freeness $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$ is called *perfect* if $k \leq 3d + 1$, the tuple $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ is a self-covering sequence, and $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \{0, 1\}$ for every $(s, t) \in U$.

Proposition 8.3. *The trace language of a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ is not context-free if, and only if, $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ admits a perfect witness of non-context-freeness.*

Proof (Sketch). We show that every witness of non-context-freeness can be transformed into a perfect one. The proposition then follows from Theorem 8.2. Consider a witness of non-context-freeness $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$, and assume, w.l.o.g., that U is minimal with respect to inclusion. We can show that U contains

---

[1] Given a matching pair $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ and an index i such that $\boldsymbol{v}_2(i) \leq 0$, it holds that $i \in \|\mathsf{exc}(\boldsymbol{v}_1, \boldsymbol{v}_2)\|^+$ if, and only if, $\boldsymbol{v}_1(i) \cdot \boldsymbol{v}_2(j) < \boldsymbol{v}_1(j) \cdot \boldsymbol{v}_2(i)$ for some index $j \neq i$.

at most two pairs for each index $i \in \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+$, hence, the support $S = \{s, t \mid (s, t) \in U\}$ of U has a cardinality of at most $3d$. Obviously, we may transform the witness by keeping only the pumping segments σ_i for $i \in S \cup \{k\}$. The remaining pumping segments are merged together with the words u_i that surround them. By construction, the resulting witness of non-context-freeness is a self-covering sequence with at most $3d + 1$ pumping segments since $|S| \leq 3d$. It remains to enforce the ratios to be in $\{0, 1\}$. Pick a pair $(s, t) \in U$ such that $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t))$ is a positive rational number, written $\frac{p}{q}$. Observe that

$$\mathsf{rat}(n_1 \boldsymbol{v}_1, n_2 \boldsymbol{v}_2) = \frac{n_1}{n_2} \cdot \mathsf{rat}(\boldsymbol{v}_1, \boldsymbol{v}_2)$$
$$\mathsf{exc}(n_1 \boldsymbol{v}_1, n_2 \boldsymbol{v}_2) = n_1 \cdot \mathsf{exc}(\boldsymbol{v}_1, \boldsymbol{v}_2)$$

for every matching pair $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ and positive natural numbers n_1 and n_2. So we define $\sigma'_s = \sigma_s^q$, $\sigma'_t = \sigma_t^p$ and $\sigma'_i = \sigma_i^n$ for $i \notin \{s, t\}$, where n is equal to p or q. We derive from Lemma 2.2 that there exists $u'_1, \ldots, u'_k$ such that $(u'_1, \sigma'_1, \ldots, u'_k, \sigma'_k, U)$ is a witness of non-context-freeness. This transformation guarantees that $\mathsf{rat}(\Delta(\sigma'_s), \Delta(\sigma'_t)) = 1$, however, it may also change the ratios of other pairs involving s (if $n = p$) or t (if $n = q$). Still, as $(\sigma_1, \ldots, \sigma_k, U)$ is a matching scheme, it is possible to process the pairs $(s, t) \in U$ in an appropriate order that prevents such conflicts. □

Example 8.4. Consider the VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\mathrm{init}} \rangle$ given by $\boldsymbol{A} = \{\boldsymbol{a}, \boldsymbol{b}\}$ and $\boldsymbol{c}_{\mathrm{init}} = (2, 2)$, where $\boldsymbol{a} = (-2, 3)$ and $\boldsymbol{b} = (3, -2)$. The tuple $(\varepsilon, \boldsymbol{ab}, \varepsilon, \boldsymbol{a}, \varepsilon, \boldsymbol{b}, U)$, with $U = \{(1, 2), (1, 3)\}$, is a witness of non-context-freeness. This witness is not perfect since $\mathsf{rat}(\Delta(\boldsymbol{ab}), \Delta(\boldsymbol{a})) = \mathsf{rat}((1, 1), (-2, 3)) = \frac{1}{2}$. Replacing $\boldsymbol{ab}$ by $\boldsymbol{abab}$ in the witness makes it perfect. □

We now explain how to encode by a formula in our logic the conditions of perfect witnesses of non-context-freeness. Consider a positive natural number k and a nested relation U on $\{1, \ldots, k\}$. Firstly, we express that $(\Delta(\sigma_s), \Delta(\sigma_t))$ is a matching pair with ratio in $\{0, 1\}$ for every $(s, t) \in U$, by the following formula:

$$\bigwedge_{(s,t) \in U} \left(\bigwedge_{i=1}^{d} \boldsymbol{\delta}_s(i) \geq 0 \ \wedge \ \bigvee_{i=1}^{d} -\boldsymbol{\delta}_t(i) \geq 1 \ \wedge \ (\rho_0(s, t) \vee \rho_1(s, t)) \right)$$

where $\rho_0(s, t)$ and $\rho_1(s, t)$ are formulas, expressible in our logic, specifying that the matching pair $(\Delta(\sigma_s), \Delta(\sigma_t))$ has ratio 0 and 1, respectively.

Secondly, we encode the requirements of Definition 8.1. The condition that $\Delta(\sigma_k) \not\geq \boldsymbol{0}$ is expressed by the formula $\bigvee_{i=1}^{d} -\boldsymbol{\delta}_k(i) \geq 1$. For the encoding of the condition $\|\Delta(\sigma_k)\|^- \subseteq \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+$, we exploit the property that the ratio of each matching pair $(\Delta(\sigma_s), \Delta(\sigma_t))$ is either 0 or 1, as follows:

$$\bigwedge_{i=1}^{d} \left(\boldsymbol{\delta}_k(i) \geq 0 \ \vee \bigvee_{(s,t) \in U} (\rho_0(s, t) \wedge \boldsymbol{\delta}_s(i) \geq 1) \vee (\rho_1(s, t) \wedge \boldsymbol{\delta}_s(i) + \boldsymbol{\delta}_t(i) \geq 1) \right)$$

13

The last condition of Definition 8.1 is expressed by the following formula:

$$\bigwedge_{(s,t)\in U, t<k}\left(\bigvee_{(r,t)\in U, r\leq s}\bigwedge_{i=1}^{d}\boldsymbol{\delta}_t(i)\geq 0 \ \vee \ \boldsymbol{\delta}_r(i)\geq 1\right)$$

Let $\varphi(k,U)$ be the conjunction of the above formulas, and let ψ denote the disjunction of all $\varphi(k,U)$ where $1 \leq k \leq 3d+1$ and U is a nested relation on $\{1,\ldots,k\}$. As intended, the formula ψ expresses non-context-freeness of the trace language. We derive the complexity of the context-freeness problem for VAS from the analysis of our logic developed in the previous sections.

Theorem 8.5. *The context-freeness problem for VAS is* ExpSpace-*complete.*

Proof. By construction, $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}}\rangle$ admits a perfect witness of non-context-freeness if, and only if, $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}}\rangle$ satisfies ψ. It follows from Proposition 8.3 that the trace language of $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}}\rangle$ is not context-free if, and only if, $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}}\rangle$ satisfies ψ. It is readily seen that $|\psi|$ is at most exponential in the dimension d, and that the conjunction rank of ψ is bounded by a polynomial in d. We derive from Theorem 5.2, with the same arguments as in Corollary 7.2, that the context-freeness problem for VAS can be solved in exponential space. The exponential space lower bound is obtained by a reduction from the boundedness problem for VAS. $\square$

9 Discussion and Future Work

We introduced a logic that can express positive Boolean combinations of linear relations among the displacements of pumping segments in self-covering sequences. We showed that if a VAS satisfies a formula, there are witnessing self-covering sequences whose size is at most doubly-exponential in the size of the VAS and the formula. This gives an exponential space upper bound for the model-checking problem for our logic, which in turn gives an exponential space upper bound for the context-freeness problem.

Yen introduced a logic similar to ours in [17], interpreted over all traces instead of self-covering sequences like we do. Atig and Habermehl showed in [1] that the problem of checking whether there is a trace satisfying a given formula in Yen's path logic is in the class $\mathcal{C}_{\text{RP}}$ (i.e., equivalent to the reachability problem). They also give a fragment of Yen's path logic that can be checked in exponential space. This fragment imposes the condition that the total displacement of the words under consideration is greater than or equal to $\boldsymbol{0}$, which is incomparable with our restriction to self-covering sequences and also incompatible with witnesses of non-context-freeness.

A logic similar to ours was introduced by Demri in [3], interpreted over self-covering sequences. In place of $t \geq n$ in our logic, the conditions allowed in [3] can constrain a variable to be inside any interval of integers. However, we allow combining $\Delta(\sigma_1), \ldots, \Delta(\sigma_k)$ in a single term, which is not allowed in [3]. Hence,

the two logics are incomparable. The inability of the logic in [3] to combine $\Delta(\sigma_1), \ldots, \Delta(\sigma_k)$ in a single term renders it unable to express the presence of witnesses of non-context-freeness.

Blockelet and Schmitz introduced in [2] a fragment of computational tree logic enriched with formulas in Presburger arithmetic for expressing properties of coverability graphs. An exponential space upper bound is provided for a fragment of this logic by imposing a so-called *eventually increasing* condition that is similar to the one imposed in [1], but for trees instead of paths. Again, this condition is incompatible with witnesses of non-context-freeness.

It will be interesting to see if the techniques used in the above collection of incomparable logics can be unified to define a logic that extends all of them and that can still be checked in exponential space.

References

1. M. F. Atig and P. Habermehl. On yen's path logic for Petri nets. *Int. J. Found. Comput. Sci.*, 22(4):783–799, 2011.
2. M. Blockelet and S. Schmitz. Model checking coverability graphs of vector addition systems. In *Proc. MFCS*, volume 6907 of *LNCS*, pages 108–119, 2011.
3. S. Demri. On selective unboundedness of vass. In *Proc. INFINITY*, volume 39 of *EPTCS*, pages 1–15, 2010.
4. J. Esparza and M. Nielsen. Decidability issues for Petri nets - a survey. *Bulletin of the EATCS*, 52:244–262, 1994.
5. R. M. Karp and R. E. Miller. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2):147 – 195, 1969.
6. S. R. Kosaraju. Decidability of reachability in vector addition systems. In *Proc. STOC*, pages 267–281. ACM, 1982.
7. J. Leroux. Vector addition system reversible reachability problem. *Logical Methods in Computer Science*, 9(1), 2013.
8. J. Leroux, V. Penelle, and G. Sutre. On the context-freeness problem for vector addition systems. In *Proc. LICS*. IEEE, 2013. To appear.
9. R. J. Lipton. The reachability problem requires exponential space. Technical Report 62, Yale University, 1976.
10. E. W. Mayr. An algorithm for the general Petri net reachability problem. In *Proc. STOC*, pages 238–246. ACM, 1981.
11. E. W. Mayr and A. R. Meyer. The complexity of the finite containment problem for Petri nets. *J. ACM*, 28(3):561–576, July 1981.
12. L. Pottier. Minimal solutions of linear diophantine systems: Bounds and algorithms. In *Proc. RTA*, volume 488 of *LNCS*, pages 162–173, 1991.
13. C. Rackoff. The covering and boundedness problems for vector addition systems. *Theoretical Computer Science*, 6(2):223–231, 1978.
14. S. R. Schwer. The context-freeness of the languages associated with vector addition systems is decidable. *Theor. Comput. Sci.*, 98(2):199–247, 1992.
15. R. Valk and M. Jantzen. The residue of vector sets with applications to decidability problems in Petri nets. *Acta Inf.*, 21:643–674, 1985.
16. R. Valk and G. Vidal-Naquet. Petri nets and regular languages. *Journal of Computer and System Sciences*, 23(3):299–325, 1981.
17. H-C. Yen. A unified approach for deciding the existence of certain Petri net paths. *Inf. Comput.*, 96(1):119–137, 1992.

A Proofs of Section 2

The following lemma will be used in the proof of Lemma 2.2.

Lemma A.1. *Let $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ be a sequence of vectors in $\mathbb{Z}^d$ such that $\|\boldsymbol{v}_h\|^- \subseteq \bigcup_{j=1}^{h-1} \|\boldsymbol{v}_j\|^+$ for every $h \in \{1, \ldots, k\}$. There exist positive integers $p_1, \ldots, p_k$ such that $\boldsymbol{x}_h = \sum_{j=1}^{h} p_j \boldsymbol{v}_j$ satisfies $\boldsymbol{x}_h \geq \boldsymbol{0}$ and $\|\boldsymbol{x}_h\|^+ = \bigcup_{j=1}^{h} \|\boldsymbol{v}_j\|^+$ for every $h \in \{1, \ldots, k\}$.*

Proof. The lemma is proved by induction over k. The case $k = 0$ is immediate. Assume the lemma proved for some $k \in \mathbb{N}$ and let us consider a sequence $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k+1})$ of vectors in $\mathbb{Z}^d$ such that $\|\boldsymbol{v}_h\|^- \subseteq \bigcup_{j=1}^{h-1} \|\boldsymbol{v}_j\|^+$ for every $h \in \{1, \ldots, k+1\}$. By induction, there exist positive integers $p_1, \ldots, p_k$ such that $\boldsymbol{x}_h = \sum_{j=1}^{h} p_j \boldsymbol{v}_j$ satisfies $\boldsymbol{x}_h \geq \boldsymbol{0}$ and $\|\boldsymbol{x}_h\|^+ = \bigcup_{j=1}^{h} \|\boldsymbol{v}_j\|^+$ for every $h \in \{1, \ldots, k\}$. Since $\|\boldsymbol{v}_{k+1}\|^- \subseteq \bigcup_{j=1}^{k} \|\boldsymbol{v}_j\|^+$ and this last set is equal to $\|\boldsymbol{x}_k\|^+$, we deduce that there exists $n \in \mathbb{N}_{>0}$ such that $\boldsymbol{x}_{k+1} = n\boldsymbol{x}_k + \boldsymbol{v}_{k+1}$ satisfies $\boldsymbol{x}_{k+1} \geq \boldsymbol{0}$ and $\|\boldsymbol{x}_{k+1}\|^+ = \bigcup_{j=1}^{k+1} \|\boldsymbol{v}_j\|^+$. The induction is proved by considering $p'_1, \ldots, p'_{k+1}$ defined by $p'_{k+1} = 1$ and $p'_h = np_h$ for every $h \in \{1, \ldots, k\}$. $\square$

Lemma 2.2. *A sequence $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ of words is self-covering for a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ if, and only if, $u_1\sigma_1 \ldots u_k\sigma_k$ is a trace and for every $n \in \mathbb{N}$, there exist $n_1, \ldots, n_k \geq n$ such that $u_1\sigma_1^{n_1} \cdots u_k\sigma_k^{n_k}$ is a trace.*

Proof. Assume first that $u_1\sigma_1 \ldots u_k\sigma_k$ is a trace and for every $n \in \mathbb{N}$, there exist $n_1, \ldots, n_k \geq n$ such that $u_1\sigma_1^{n_1} \cdots u_k\sigma_k^{n_k}$ is a trace. Let $h \in \{1, \ldots, k\}$ and $i \notin \bigcup_{j=1}^{h-1} \|\Delta(\sigma_j)\|^+$. We prove that $\Delta(\sigma_h)(i) \geq 0$ by introducing a positive natural number n such that $\boldsymbol{c}_{init}(i) + \Delta(u_1)(i) + \cdots + \Delta(u_h)(i) < n$. By definition, there exist $n_1, \ldots, n_k \geq n$ such that $u_1\sigma_1^{n_1} \ldots u_h\sigma_h^{n_h}$ is a trace, since this word is a prefix of the trace $u_1\sigma_1^{n_1} \ldots u_k\sigma_k^{n_k}$. Hence, $\boldsymbol{c}_{init} + \Delta(u_1) + \cdots + \Delta(u_h) + n_1\Delta(\sigma_1) + \cdots + n_h\Delta(\sigma_h) \geq \boldsymbol{0}$. Since $\Delta(\sigma_j)(i) \leq 0$ for every $j \in \{1, \ldots, h-1\}$ we derive the inequality $n_h\Delta(\sigma_h)(i) > -n$. Thus $\Delta(\sigma_h)(i) > -1$. We get the inequality $\Delta(\sigma_h)(i) \geq 0$ which proves that $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ is a self-covering sequence.

Conversely, let us assume that $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ is a self-covering sequence. Let us consider a run of the following form where $\boldsymbol{c}'_0 = \boldsymbol{c}_{init}$:

$$\boldsymbol{c}'_0 \xrightarrow{u_1} \boldsymbol{c}_1 \xrightarrow{\sigma_1} \boldsymbol{c}'_1 \cdots \xrightarrow{u_k} \boldsymbol{c}_k \xrightarrow{\sigma_k} \boldsymbol{c}'_k$$

Assume that $\|\Delta(\sigma_h)\|^- \subseteq \bigcup_{j=1}^{h-1} \|\Delta(\sigma_j)\|^+$ for every $h \in \{1, \ldots, k\}$. Lemma A.1 shows that there exists $p_1, \ldots, p_k \in \mathbb{N}_{>0}$ such that $\boldsymbol{x}_h = \sum_{j=1}^{h} p_j \Delta(\sigma_j)$ satisfies $\boldsymbol{x}_h \geq \boldsymbol{0}$ for every $h \in \{0, \ldots, k\}$.

Note that $\boldsymbol{x}_{h-1} + p_h\Delta(\sigma_h) \geq \boldsymbol{0}$ since this vector is equal to $\boldsymbol{x}_h$. As $\boldsymbol{x}_{h-1} \geq \boldsymbol{0}$ we deduce that $\boldsymbol{x}_{h-1} + p\Delta(\sigma_h) \geq \boldsymbol{0}$ for every $0 \leq p \leq p_h$. As there exists a run from $\boldsymbol{c}_h$ labeled by σ_h, by monotony we deduce that there exists a run from $\boldsymbol{c}_h + \boldsymbol{x}_{h-1} + p\Delta(\sigma_h)$ labeled by the same word. Thus:

$$\boldsymbol{c}_h + \boldsymbol{x}_{h-1} + p\Delta(\sigma_h) \xrightarrow{\sigma_h} \boldsymbol{c}_h + \boldsymbol{x}_{h-1} + (p+1)\Delta(\sigma_h)$$

16

We deduce that that there exists a run $\boldsymbol{c}_h + \boldsymbol{x}_{h-1} \xrightarrow{\sigma_h^{p_h}} \boldsymbol{c}_h + \boldsymbol{x}_h$. By induction over $m \in \mathbb{N}$, we get $\boldsymbol{c}_h + m\boldsymbol{x}_{h-1} \xrightarrow{\sigma_j^{mp_h}} \boldsymbol{c}_h + m\boldsymbol{x}_h$. We get the following run:

$$\boldsymbol{c}_0' + m\boldsymbol{x}_0 \xrightarrow{u_1} \boldsymbol{c}_1 + m\boldsymbol{x}_0 \xrightarrow{\sigma_1^{mp_1+1}} \boldsymbol{c}_1' + m\boldsymbol{x}_1 \cdots \xrightarrow{u_k} \boldsymbol{c}_k + m\boldsymbol{x}_{k-1} \xrightarrow{\sigma_k^{mp_k+1}} \boldsymbol{c}_k' + m\boldsymbol{x}_k$$

Finally, for every $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $mp_j + 1 \geq n$ for every j. We introduce $n_j = mp_j + 1$. We have proved the lemma since $\boldsymbol{x}_0 = \boldsymbol{0}$. $\qquad\square$

B   Proofs of Section 5

Lemma 5.4. *Consider a run* $\boldsymbol{c}_{init} \xrightarrow{u_1} \boldsymbol{c}_1 \xrightarrow{\sigma_1} \boldsymbol{c}_1' \to \cdots \xrightarrow{u_k} \boldsymbol{c}_k \xrightarrow{\sigma_k} \boldsymbol{c}_k'$ *of* $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$*, with* $|\sigma_1| + \cdots + |\sigma_k| \leq l$*. Then there are words* $u_1', \ldots, u_k'$ *such that* $u_1'\sigma_1 \cdots u_k'\sigma_k$ *is a trace and* $|u_1'| + \cdots + |u_k'| \leq (2l\|\boldsymbol{A}\|_\infty)^{((d+1)k+1)!}$.

Proof. The main idea here is to combine k paths into a single path of a suitably constructed VAS with additional indices. For a d-dimensional VAS $\boldsymbol{A}$, following is an illustration of the $((d+1)k)$-dimensional VAS $\boldsymbol{A}^{k\downarrow}$, which is formalized in the definition that follows.

$$
\begin{bmatrix} \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \end{bmatrix} \text{ in } \boldsymbol{A} \Rightarrow
\begin{bmatrix} \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \vdots \\ \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \boldsymbol{0} \end{bmatrix},
\begin{bmatrix} \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \vdots \\ \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \boldsymbol{0} \\ \boldsymbol{0} \end{bmatrix}, \ldots,
\begin{bmatrix} \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \vdots \\ \boldsymbol{0} \\ \boldsymbol{0} \\ \boldsymbol{0} \end{bmatrix} \text{ in } \boldsymbol{A}^{k\downarrow}
$$

The last k indices of $\boldsymbol{A}^{k\downarrow}$ are thought of as grouped into one, which are left unchanged by all actions. The rest of the $(k \cdot d)$ indices are thought of as being divided into k groups of d indices each. An action $\boldsymbol{a}$ of $\boldsymbol{A}$ gives rise to k actions $\boldsymbol{a}^{k\downarrow k}, \ldots, \boldsymbol{a}^{k\downarrow 1}$ in $\boldsymbol{A}^{k\downarrow}$. The action $\boldsymbol{a}^{k\downarrow k}$ duplicates the action of $\boldsymbol{a}$ on the first k groups of indices. The action $\boldsymbol{a}^{k\downarrow(k-1)}$ duplicates the action of $\boldsymbol{a}$ on the first $(k-1)$ groups of indices, leaving the rest unchanged and so on.

Definition B.1. *For* $\boldsymbol{a} \in \mathbb{Z}^d$ *and* $j \in \{1, \ldots, k\}$*,* $\boldsymbol{a}^{(k\downarrow j)}$ *is the* $((d+1)k)$-*dimensional vector that results in* $\boldsymbol{a}$ *when projected to the indices* $\{(i-1)d +$

$1, \ldots, (i-1)d + d\}$ *for any i between 1 and j, and has the value 0 in all other indices. Given $\boldsymbol{A} \subseteq \mathbb{Z}^d$ and $1 \leq j \leq k$, $\boldsymbol{A}^{(k\downarrow j)} = \{\boldsymbol{a}^{(k\downarrow j)} \mid \boldsymbol{a} \in \boldsymbol{A}\}$ and $\boldsymbol{A}^{(k\downarrow)} = \cup_{1 \leq j \leq k} \boldsymbol{A}^{(k\downarrow j)}$.*

For a word σ, let $\boldsymbol{c}_\sigma$ be the unique minimum configuration that enables σ. For every j between 1 and k, let $\boldsymbol{a}_j$ be the $((d+1)k)$-dimensional vector such that

1. $\boldsymbol{a}_j(kd + j) = 1$,
2. when $\boldsymbol{a}_j$ is projected to the indices $\{(i-1)d + 1, \ldots, (i-1)d + d\}$ where $1 \leq i \leq k - j$, the result is $\Delta(\sigma_j)$ and
3. $\boldsymbol{a}_j$ has the value 0 in all other indices.

Let $u_j^{k\downarrow k-j+1}$ be the word obtained from u_j by replacing each action $\boldsymbol{a}$ of u_j with $\boldsymbol{a}^{k\downarrow k-j+1}$. Let $\boldsymbol{c}_{\text{init}}^{k+d}$ be the vector obtained by adjoining k copies of $\boldsymbol{c}_{\text{init}}$ and the d-dimensional vector $\langle 0, \ldots, 0 \rangle$. Let $\boldsymbol{c}$ be the configuration obtained by adjoining the vectors $\boldsymbol{c}_{\sigma_k}, \ldots, \boldsymbol{c}_{\sigma_1}, 1^d$, where 1^d is the d-dimensional vector all of whose values are 1. We have by definition, $\boldsymbol{c}_{\text{init}}^{k+d} \xrightarrow{u_1^{k\downarrow k} \boldsymbol{a}_1 u_2^{k\downarrow k-1} \boldsymbol{a}_2 \cdots u_k^{k\downarrow 1} \boldsymbol{a}_k} \boldsymbol{c}'$ such that $\boldsymbol{c}' \geq \boldsymbol{c}$. Following is an illustration, where u_1^k is written as $\langle u_1, u_1, \ldots, u_1, 0, 0, \ldots, 0 \rangle$, $\boldsymbol{a}_1$ is written as $\langle \Delta(\sigma_1), \Delta(\sigma_1), \ldots, \boldsymbol{0}, 1, 0, \ldots, 0 \rangle$ and so on.

$$
\begin{bmatrix}
\boldsymbol{c}_{\text{init}} \\
\boldsymbol{c}_{\text{init}} \\
\vdots \\
\boldsymbol{c}_{\text{init}} \\
0 \\
0 \\
\vdots \\
0
\end{bmatrix}
\begin{matrix}
u_1 & \Delta(\sigma_1) & u_2 & \Delta(\sigma_2) & & u_k & \boldsymbol{0} \\
u_1 & \Delta(\sigma_1) & u_2 & \Delta(\sigma_2) & \cdots & \boldsymbol{0} & \boldsymbol{0} \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\
u_1 & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & & \boldsymbol{0} & \boldsymbol{0} \\
0 & 1 & 0 & 0 & & 0 & 0 \\
0 & 0 & 0 & 1 & & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & 0 & & 0 & 1
\end{matrix}
\begin{bmatrix}
\geq \boldsymbol{c}_{\sigma_k} \\
\geq \boldsymbol{c}_{\sigma_{k-1}} \\
\vdots \\
\geq \boldsymbol{c}_{\sigma_1} \\
1 \\
1 \\
\vdots \\
1
\end{bmatrix}
$$

By Lemma 5.3, we infer that there is a sub-word $u_1'^{k\downarrow k} \boldsymbol{a}_1 u_2'^{k\downarrow k-1} \boldsymbol{a}_2 \cdots u_k'^{k\downarrow 1} \boldsymbol{a}_k$ of $u_1^{k\downarrow k} \boldsymbol{a}_1 u_2^{k\downarrow k-1} \boldsymbol{a}_2 \cdots u_k^{k\downarrow 1} \boldsymbol{a}_k$ of length at most $(2l\|\boldsymbol{A}\|_\infty)^{((d+1)k+1)!}$ such that $\boldsymbol{c}_{\text{init}}^{k+d} \xrightarrow{u_1'^{k\downarrow k} \boldsymbol{a}_1 u_2'^{k\downarrow k-1} \boldsymbol{a}_2 \cdots u_k'^{k\downarrow 1} \boldsymbol{a}_k} \boldsymbol{c}''$ and $\boldsymbol{c}'' \geq \boldsymbol{c}$. The actions $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ will be definitely present in the sub-word since they are the only ones that can increase the value of the indices $kd + 1, \ldots, kd + k$ respectively. For each j between 1 and k, let u_j' be the action obtained from $u_j'^{k\downarrow k-j+1}$ by replacing each action $\boldsymbol{a}^{k\downarrow k-j+1}$ of $u_j'^{k\downarrow k-j+1}$ by $\boldsymbol{a}$. We have $\boldsymbol{c}_{\text{init}} \xrightarrow{u_1' \sigma_1} \boldsymbol{c}_1'' \xrightarrow{u_2' \sigma_2} \cdots \xrightarrow{u_k' \sigma_k} \boldsymbol{c}_k''$. Hence the lemma is proved. $\qquad\square$

C Proofs of Section 6

Lemma 6.3. *Let $\boldsymbol{Z}$ be a $r \times d$ integer matrix and let $\boldsymbol{b} \in \mathbb{Z}^r$ be a vector. The set of all integer vectors $\boldsymbol{\rho}$ such that $\boldsymbol{Z}\boldsymbol{\rho} \geq \boldsymbol{b}$ is a finite union of sets of the form $\boldsymbol{p}_0 + \mathbb{N}\boldsymbol{p}_1 + \cdots + \mathbb{N}\boldsymbol{p}_m$, where $m \in \mathbb{N}$ and $\boldsymbol{p}_0, \boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ are integer vectors such that $\|\boldsymbol{p}_0\|_1, \|\boldsymbol{p}_1\|_1, \ldots, \|\boldsymbol{p}_m\|_1 \leq (2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{b}\|_\infty)^r$.*

Proof. For two matrices $\boldsymbol{Z_1}, \boldsymbol{Z}_2$ of the same dimensions, the Hadamard product $\boldsymbol{Z_1} \circ \boldsymbol{Z}_2$ is a matrix of the same dimensions whose elements are $(\boldsymbol{Z_1} \circ \boldsymbol{Z}_2)(i,j) = \boldsymbol{Z}_1(i,j) \cdot \boldsymbol{Z}_2(i,j)$ for all i,j. Let $\boldsymbol{\pi} \in \{-1,+1\}^d$ (we think of π as a vector that permutes the sign of some of its indices). Let $\boldsymbol{\pi}^r$ be the $r \times d$ matrix such that every row of $\boldsymbol{\pi}^r$ is equal to $\boldsymbol{\pi}$.

$$\{\boldsymbol{\rho} \in \mathbb{Z}^d \mid \boldsymbol{Z}\boldsymbol{\rho} \geq \boldsymbol{b}\}$$
$$= \bigcup_{\boldsymbol{\pi} \in \{-1,+1\}^d} \{\boldsymbol{\pi} \circ \boldsymbol{\rho}' \mid \boldsymbol{\rho}' \in \mathbb{N}^d, [\boldsymbol{\pi}^r \circ \boldsymbol{Z}]\rho' \geq \boldsymbol{b}\} \qquad (3)$$

Let $-\boldsymbol{I}_r$ be the $r \times r$ identity matrix multiplied by -1. Let $\boldsymbol{\theta}$ be a natural number vector of dimension r. Let t be a temporary variable ranging over the set of natural numbers. Let $[\boldsymbol{\pi}^r \circ \boldsymbol{Z}; -\boldsymbol{I}_r; -\boldsymbol{b}]$ be the matrix of r rows obtained by adjoining $\boldsymbol{\pi}^r \circ \boldsymbol{Z}, -\boldsymbol{I}_r$ and $-\boldsymbol{b}$. We have the following equality.

$$\{\boldsymbol{\rho}' \in \mathbb{N}^d, [\boldsymbol{\pi}^r \circ \boldsymbol{Z}]\rho' \geq \boldsymbol{b}\} =$$
$$\{\boldsymbol{\rho}' \in \mathbb{N}^d \mid [\boldsymbol{\pi}^r \circ \boldsymbol{Z}; -\boldsymbol{I}_r; -\boldsymbol{b}] \begin{bmatrix} \boldsymbol{\rho}' \\ \boldsymbol{\theta} \\ t \end{bmatrix} = \boldsymbol{0}, \boldsymbol{\theta} \in \mathbb{N}^r, t = 1\} \qquad (4)$$

From [12, Theorem 1], we get

$$\left\{ \langle \boldsymbol{\rho}', \boldsymbol{\theta}, t \rangle \in \mathbb{N}^{d+r+1} \mid [\boldsymbol{\pi}^r \circ \boldsymbol{Z}; -\boldsymbol{I}_r; -\boldsymbol{b}] \begin{bmatrix} \boldsymbol{\rho}' \\ \boldsymbol{\theta} \\ t \end{bmatrix} = \boldsymbol{0} \right\} = \sum_{\boldsymbol{q} \in \mathcal{C}_\pi} \mathbb{N}\boldsymbol{q} \qquad (5)$$

where $\mathcal{C}_\pi \subseteq \mathbb{N}^{d+r+1}$ is a finite set of natural number vectors such that $\|\mathcal{C}_\pi\|_1 \leq (1 + \|[\boldsymbol{Z}; -\boldsymbol{I}_r; -\boldsymbol{b}]\|_{1,\infty})^r$. Let $\mathcal{C}_\pi^1 = \{\boldsymbol{\rho}' \in \mathbb{N}^d \mid \exists \boldsymbol{\theta} \in \mathbb{N}^r, \langle \boldsymbol{\rho}', \boldsymbol{\theta}, 1 \rangle \in \mathcal{C}_\pi\}$ and $\mathcal{C}_\pi^0 = \{\boldsymbol{\rho}' \in \mathbb{N}^d \mid \exists \boldsymbol{\theta} \in \mathbb{N}^r, \langle \boldsymbol{\rho}', \boldsymbol{\theta}, 0 \rangle \in \mathcal{C}_\pi\}$. We get the following from (3).

$$\{\boldsymbol{\rho} \in \mathbb{Z}^d \mid \boldsymbol{Z}\boldsymbol{\rho} \geq \boldsymbol{b}\}$$
$$= \bigcup_{\boldsymbol{\pi} \in \{-1,+1\}^d} \{\boldsymbol{\pi} \circ \boldsymbol{\rho}' \mid \boldsymbol{\rho}' \in \mathbb{N}^d, [\boldsymbol{\pi}^r \circ \boldsymbol{Z}]\rho' \geq \boldsymbol{b}\}$$
$$= \bigcup_{\boldsymbol{\pi} \in \{-1,+1\}^d, \boldsymbol{p}' \in \mathcal{C}_\pi^1} \{\boldsymbol{\pi} \circ \boldsymbol{p}' + \sum_{\boldsymbol{q}' \in \mathcal{C}_\pi^0} \mathbb{N}(\boldsymbol{\pi} \circ \boldsymbol{q}')\}$$

Since $\|[\boldsymbol{Z}; -\boldsymbol{I}_r; -\boldsymbol{b}]\|_{1,\infty} \leq \|Z\|_{1,\infty} + 1 + \|\boldsymbol{b}\|_\infty$, we get $\|\mathcal{C}_\pi^1\|_1, \|\mathcal{C}_\pi^0\|_1 \leq (2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{b}\|_\infty)^r$ and this proves the lemma. $\qquad \square$

Lemma 6.4. *Let $\boldsymbol{A} \subseteq \mathbb{Z}^d$ be a finite set and $\boldsymbol{x} \in \mathbb{N}_\omega^d$ be an extended configuration. Suppose there is a word $\sigma \in \boldsymbol{A}^*$ such that $\boldsymbol{x} \xrightarrow{\sigma} \boldsymbol{x}$ and $\boldsymbol{Z}\Delta(\sigma) \geq \boldsymbol{n}$, where $\boldsymbol{Z} \in \mathbb{Z}^{r \times d}$ is an integer matrix with r rows, d columns and $\boldsymbol{n} \in \mathbb{N}^r$ is a vector of natural numbers. Then there is a word $\sigma' \in \boldsymbol{A}^*$ such that $\boldsymbol{x} \xrightarrow{\sigma'} \boldsymbol{x}$, $\boldsymbol{Z}\Delta(\sigma') \geq \boldsymbol{n}$ and $|\sigma'| \leq (\|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty)^{rc_2^{d^3}}$ for some constant c_2.*

Proof (Continued).

$$x = (1 + 2\|\widetilde{\boldsymbol{A}}\|_\infty)(1 + \|\boldsymbol{c}''\|_\infty + \|\Delta u'\|_\infty)$$
$$\le (1 + 2\tilde{a})(1 + \|\boldsymbol{c}'\|_\infty + \|\boldsymbol{p}_0\|_\infty + \|\boldsymbol{p}_0\|_\infty)$$
$$\le (1 + 2\tilde{a})(1 + \|\boldsymbol{c}'\|_\infty + 2\tilde{a})$$
$$\le 2(1 + 2\tilde{a} + \|\boldsymbol{c}'\|_\infty)$$
$$\le 2\left[1 + 2\tilde{a} + (102d^2\tilde{a}^2)^{(15d^{d+2})^{d+2}}\right]$$
$$\le 2\left[(104d^2\tilde{a}^2)^{(15d^{d+2})^{d+2}}\right]$$
$$\le (208d^2\tilde{a}^2)^{(15d^{d+2})^{d+2}}$$
$$\le (30\tilde{a})^{60^{10d^3}}$$

$$\tilde{a} = \|\widetilde{\boldsymbol{A}}\|_\infty = \max\{\|\boldsymbol{A}\|_\infty, \|\boldsymbol{p}_0\|_\infty, \|\boldsymbol{p}_1\|_\infty, \ldots, \|\boldsymbol{p}_m\|_\infty\}$$
$$\le \max\{\|\boldsymbol{A}\|_\infty, \|\boldsymbol{p}_0\|_1, \|\boldsymbol{p}_1\|_1, \ldots, \|\boldsymbol{p}_m\|_1\}$$
$$\le \max\{\|\boldsymbol{A}\|_\infty, (2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{n}'\|_\infty)^{r+2d}\}$$
$$\le (2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty)^{r+2d}$$

$$x \le (30\tilde{a})^{60^{10d^3}}$$
$$\le (30(2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty))^{(r+2d)60^{10d^3}}$$

$$|\sigma'| \le |u''| \le 17d^2 x^{15d^{d+2}}$$
$$\le 17d^2(30(2 + \|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty))^{(r+2d)15d^{d+2}60^{10d^3}}$$
$$\le [c_3(\|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty)]^{rc_4^{c_5 d^3}}$$

for suitably chosen constants c_3, c_4 and c_5.

If $\|\boldsymbol{Z}\|_{1,\infty} = 0$ (resp. $\|\boldsymbol{A}\|_\infty = 0$), all entries of $\boldsymbol{Z}$ (resp. $\boldsymbol{A}$) are zero, which is a trivial case. Hence, we can assume that $\|\boldsymbol{Z}\|_{1,\infty}, \|\boldsymbol{A}\|_\infty \ge 1$ and hence $\|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty \ge 2$. Hence, we can conclude that $|\sigma'| \le (\|\boldsymbol{Z}\|_{1,\infty} + \|\boldsymbol{A}\|_\infty + \|\boldsymbol{n}\|_\infty)^{rc_2^{d^3}}$ for a suitably chosen constant c_2. $\qquad\square$

D   Proofs of Section 7

Lemma 7.1. *Suppose there is a self-covering sequence $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ satisfying ϕ. Then there is a self-covering sequence $(u'_1, \sigma'_1, \ldots, u'_k, \sigma'_k)$ satisfying ϕ such that $|\sigma'_1| + \cdots + |\sigma'_k| \le (\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{r(\phi)c_1^{(d \cdot k(\phi))^3}}$ where c_1 is a constant.*

20

Proof. For each disjunctive sub-formula of ϕ, one of the disjuncts is satisfied by $u_1\sigma_1 \cdots u_k\sigma_k$. By choosing such satisfied disjuncts, we are left with a conjunction of at most $r(\phi)$ terms, where $r(\phi)$ is the conjunction rank of ϕ. In the following, we will write r in place of $r(\phi)$. Each of these r terms can be encoded as a linear inequality of the form $\boldsymbol{z} \odot \boldsymbol{\delta} \geq n$. We next add some linear inequalities that encode the conditions of a self-covering sequence. For each j between 1 and k and each i between 1 and d such that $\Delta(\sigma_j)(i) \geq 1$, add the inequality $\boldsymbol{\delta}_j(i) \geq 1$. For each j between 1 and k and each i between 1 d such that $\Delta(\sigma_j)(i) = 0$, add the inequalities $\boldsymbol{\delta}_j(i) \geq 0$ and $-\boldsymbol{\delta}_j(i) \geq 0$. The resulting linear system $\boldsymbol{Z}'\boldsymbol{\delta} \geq \boldsymbol{n}'$ has at most $r + 3kd$ rows.

Now our goal is to check the existence of words $\sigma_1, \ldots, \sigma_k$ satisfying a linear system. These are k different words of d-dimensional vectors in $\boldsymbol{A}$ whose displacements should satisfy a single linear system. We reduce this to finding a single word of $(k \cdot d)$-dimensional vectors in $\boldsymbol{A}^{(k)}$, which is shown in the example below and formalized in the definition that follows.

$$
\begin{bmatrix} \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \end{bmatrix} \text{ in } \boldsymbol{A} \Rightarrow
\begin{bmatrix} \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \\ \boldsymbol{0} \\ \\ \vdots \\ \\ \boldsymbol{0} \end{bmatrix},
\begin{bmatrix} \boldsymbol{0} \\ \\ \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \\ \\ \vdots \\ \\ \boldsymbol{0} \end{bmatrix}, \ldots,
\begin{bmatrix} \boldsymbol{0} \\ \\ \boldsymbol{0} \\ \\ \vdots \\ \\ \boldsymbol{a}(1) \\ \vdots \\ \boldsymbol{a}(d) \end{bmatrix} \text{ in } \boldsymbol{A}^{(k)}
$$

The $(k \cdot d)$ indices of $\boldsymbol{A}^{(k)}$ are thought of as being divided into k groups of d indices each. An action of $\boldsymbol{A}$ gives rise to k actions in $\boldsymbol{A}^{(k)}$. Each one of these k actions acts on one of the k groups of indices, leaving the indices of the other groups unchanged.

Definition D.1. *For $\boldsymbol{a} \in \mathbb{Z}^d$ and $j \in \{1, \ldots, k\}$, $\boldsymbol{a}^{(k,j)}$ is the $(k \cdot d)$-dimensional vector that results in $\boldsymbol{a}$ when projected to the indices $\{(j-1)d+1, \ldots, (j-1)d+d\}$ and has the value 0 in all other indices. Given $\boldsymbol{A} \subseteq \mathbb{Z}^d$ and $1 \leq j \leq k$, $\boldsymbol{A}^{(k,j)} = \{\boldsymbol{a}^{(k,j)} \mid \boldsymbol{a} \in \boldsymbol{A}\}$ and $\boldsymbol{A}^{(k)} = \cup_{1 \leq j \leq k} \boldsymbol{A}^{(k,j)}$.*

Suppose the word $u_1\sigma_1 \cdots u_k\sigma_k$ we are looking for is such that $\boldsymbol{c}_{\text{init}} \xrightarrow{u_1} \boldsymbol{c}_1 \xrightarrow{\sigma_1} \boldsymbol{c}'_1 \to \cdots \xrightarrow{u_k} \boldsymbol{c}_k \xrightarrow{\sigma_k} \boldsymbol{c}'_k$. The idea is to think of $\sigma_1, \ldots, \sigma_k$ as a single word in

$(\boldsymbol{A}^{(k)})^*$ as follows.

$$
\begin{bmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \\ \vdots \\ \boldsymbol{c}_k \end{bmatrix} \rightarrow \begin{matrix} \sigma_1 & \boldsymbol{0} & & \boldsymbol{0} \\ \boldsymbol{0} & \sigma_2 & & \boldsymbol{0} \\ \vdots & \vdots & \cdots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & & \sigma_k \end{matrix} \rightarrow \begin{bmatrix} \boldsymbol{c}'_1 \\ \boldsymbol{c}'_2 \\ \vdots \\ \boldsymbol{c}'_k \end{bmatrix} \tag{6}
$$

Let $\boldsymbol{c}_{\mathrm{init}} \xrightarrow{u_1} \boldsymbol{c}_1 \xrightarrow{\sigma_1} \boldsymbol{c}'_1 \rightarrow \cdots \xrightarrow{u_k} \boldsymbol{c}_k \xrightarrow{\sigma_k} \boldsymbol{c}'_k$. For each j between 1 and k, let $\boldsymbol{x}_j(i) = \omega$ for $i \in \cup_{1 \leq j' < j} \|\Delta(\sigma_{j'})\|^+$ and $\boldsymbol{x}_j(i) = \boldsymbol{c}_j(i)$ for $i \in \|\Delta\sigma_j\|^0 \setminus \cup_{1 \leq j' < j} \|\Delta(\sigma_{j'})\|^+$. Let $\sigma_j^{(k,j-1)}$ be the word obtained from σ_j by replacing each action $\boldsymbol{a}$ of σ_j with $\boldsymbol{a}^{(k,j-1)}$. Let $\boldsymbol{x}$ be the vector obtained by adjoining $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ and let $\sigma^{(k)} = \sigma_1^{(k,0)} \cdots \sigma_k^{(k,k-1)}$. We have $\boldsymbol{x} \xrightarrow{\sigma^{(k)}} \boldsymbol{x}$ and $\boldsymbol{Z}'\Delta(\sigma^{(k)}) \geq \boldsymbol{n}'$.

From Lemma 6.4, we infer that there is a word $\sigma' \in (\boldsymbol{A}^{(k)})^*$ such that $\boldsymbol{x} \xrightarrow{\sigma'} \boldsymbol{x}$, $\boldsymbol{Z}'\Delta(\sigma') \geq \boldsymbol{n}'$ and $|\sigma'| \leq (\|\boldsymbol{Z}'\|_{1,\infty} + \|\boldsymbol{A}^{(k)}\|_\infty + \|\boldsymbol{n}'\|_\infty)^{(r+3kd)c_2^{k^3 d^3}}$. We have $\|\boldsymbol{Z}'\|_{1,\infty}, \|\boldsymbol{n}'\|_\infty \leq \|\phi\|_1$ and $\|\boldsymbol{A}^{(k)}\|_\infty = \|\boldsymbol{A}\|_\infty$. Hence, we infer that $|\sigma'| \leq (\|\boldsymbol{A}\|_\infty + \|\phi\|_1)^{rc_1^{k^3 d^3}}$ for a suitably chosen constant c_1. For each j between 1 and k, let σ'_j be the word obtained from σ' by first restricting σ' to actions in $\boldsymbol{A}^{(k,j-1)}$ and then replacing each action $\boldsymbol{a}^{(k,j-1)}$ by $\boldsymbol{a}$. Since $\Delta(\sigma')$ is equal to the vector obtained by adjoining $\Delta(\sigma'_1), \ldots, \Delta(\sigma'_k)$ and $\boldsymbol{Z}'\Delta(\sigma') \geq \boldsymbol{n}'$, we infer that $\Delta(\sigma'_1), \ldots, \Delta(\sigma'_k)$ satisfy ϕ and the conditions for self-covering sequences.

Let $u'_0 = u_1 \sigma_1'^{\|\boldsymbol{A}\|_\infty |\sigma'_1|}$. We claim that for any j between 1 and k and any $w \in \mathbb{N}_{>0}$, there exist $n_1, \ldots, n_k \in \mathbb{N}_{>0}$ such that $\boldsymbol{c}_{\mathrm{init}} \xrightarrow{u'_0 \sigma_1'^{n_1} u_2 \sigma_2'^{n_2} \cdots u_j \sigma_j'^{n_j}} \boldsymbol{c}''_j$ such that $\boldsymbol{c}''_j(i) = \boldsymbol{x}_j(i)$ for $i \notin \|\boldsymbol{x}_j\|^\omega$ and $\boldsymbol{c}''_j(i) \geq w$ for $j \in \|\boldsymbol{x}_i\|^\omega$. The proof of the claim is by induction on j. For the base case $j = 1$, we can take $n_1 = w$. For the induction step, we let $n_j = w$ and $n_1, \ldots, n_{j-1}$ be those given by the induction hypothesis with $w + \|\boldsymbol{A}\|_\infty(|u_j| + w|\sigma'_j|)$ in place of w. This completes the induction hypothesis and hence the claim is true.

Let $\boldsymbol{c}_{\mathrm{init}} \xrightarrow{u'_0 \sigma_1'^{n_1} u_2 \sigma_2'^{n_2} \cdots u_k \sigma_k'^{n_k}} \boldsymbol{c}''_k$, where $n_1, \ldots, n_k \in \mathbb{N}_{>0}$ are those given by the claim above with $w = 1$. The lemma is proved by taking $u'_1 = u'_0 \sigma_1'^{n_1 - 1}$ and $u'_j = u_j \sigma_j'^{n_j - 1}$ for $2 \leq j \leq k$. $\qquad \square$

E Proof of Proposition 8.3

We provide, in this section, a detailed proof of Proposition 8.3. The proof is based on the following lemmas.

Lemma E.1. *For every witness of non-context-freeness* $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$, *there exists* $1 \leq j_1 < j_2 < \cdots < j_h = k$, *with* $h \leq 3d + 1$, *a binary relation* V *on* $\{1, \ldots, h\}$, *and* h *words* $v_1, \ldots, v_h$ *in* $\boldsymbol{A}^*$ *such that*

1. $(v_1, \sigma_{j_1}, \ldots, v_h, \sigma_{j_h}, V)$ *is a witness of non-context-freeness, and*
2. $(v_1, \sigma_{j_1}, \ldots, v_h, \sigma_{j_h})$ *is a self-covering sequence.*

Proof. The following notation will be used in the proof. Given a binary relation R over some set X, the *support* of R is the set of all elements in X that are related by R, formally, $\mathsf{Sup}(R) = \{s, t \mid (s, t) \in R\}$.

Let $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$ be a witness of non-context-freeness. To prove the lemma, we may assume, w.l.o.g., that U is minimal with respect to inclusion. As a first step, we show that $\mathsf{Sup}(U)$ has cardinal at most $3d$. For brevity, let us write $E = \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+$. For each index $i \in E$, there exists a pair (s_i, t_i) in U such that $\mathsf{exc}(\Delta(\sigma_{s_i}), \Delta(\sigma_{t_i}))(i) > 0$. In addition, define $r_i = \min \{s \mid (s, t_i) \in U\}$ for every $i \in E$. We prune U into the reduced binary relation

$$U_r \;=\; \{(r_i, t_i), (s_i, t_i) \mid i \in E\}$$

Observe that $U_r \subseteq U$ and that $|\mathsf{Sup}(U_r)| \leq 3d$. Since $U_r \subseteq U$, we get that $(\sigma_1, \ldots, \sigma_k, U_r)$ is a matching scheme. Moreover, since $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$ is a witness of non-context-freeness, we obtain, by construction, that

 - $\|\Delta(\sigma_k)\|^- \subseteq \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+ = \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U_r)\|^+$, and
 - $\|\Delta(\sigma_{t_i})\|^- \subseteq \|\Delta(\sigma_{r_i})\|^+$ for every $i \in E$ with $t_i < k$.

It follows that $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U_r)$ is also a witness of non-context-freeness. By minimality of U, we derive that $U = U_r$, hence, $|\mathsf{Sup}(U)| \leq 3d$.

Let us write $\mathsf{Sup}(U) \cup \{k\} = \{j_1, \ldots, j_h\}$ with $1 \leq j_1 < j_2 < \cdots < j_h = k$. Note that $3d \leq h \leq 3d + 1$. We define the binary relation V on $\{1, \ldots, h\}$ and the words $v_1, \tau_1, \ldots v_h, \tau_h$ in $\boldsymbol{A}^*$ as follows:

$$\begin{aligned}
V &= \{(s, t) \mid (j_s, j_t) \in U\} \\
\tau_i &= \sigma_{j_i} \\
v_i &= u_{j_{i-1}+1} \sigma_{j_{i-1}+1} u_{j_{i-1}+2} \cdots \sigma_{j_i - 1} u_{j_i}
\end{aligned}$$

with the convention that $j_0 = 1$. We show that $(v_1, \tau_1, \ldots, v_h, \tau_h, V)$ is a witness of non-context-freeness. It is routinely checked that $(\tau_1, \ldots, \tau_h, V)$ is a matching scheme. Let us prove that $(v_1, \tau_1, \ldots, v_h, \tau_h, V)$ fulfills the three conditions of Definition 8.1. Recall that these conditions are satisfied by $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$. Notice also that $U = \{(j_s, j_t) \mid (s, t) \in V\}$, by construction.

1. The word $v_1 \tau_1 \cdots v_h \tau_h$ is a trace since it is equal to $u_1 \sigma_1 \cdots u_k \sigma_k$, which is a trace.
2. It holds that $\|\Delta(\tau_h)\|^- = \|\Delta(\sigma_k)\|^- \neq \emptyset$. Moreover, it is routinely checked that $\mathsf{exc}(\tau_1, \ldots, \tau_h, V) = \mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)$. Hence, $\|\Delta(\tau_h)\|^- = \|\Delta(\sigma_k)\|^- \subseteq \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+ = \|\mathsf{exc}(\tau_1, \ldots, \tau_h, V)\|^+$.
3. For every $(s, t) \in V$ with $t < h$, it holds that $(j_s, j_t) \in U$ and $j_t < k$. Hence, there exists $(j_r, j_t) \in U$ such that $r \leq s$ and $\|\Delta(\sigma_{j_t})\|^- \subseteq \|\Delta(\sigma_{j_r})\|^+$. We get that $(r, t) \in V$ and $\|\Delta(\tau_t)\|^- \subseteq \|\Delta(\tau_r)\|^+$.

We conclude that $(v_1, \tau_1, \ldots, v_h, \tau_h, V)$ is a witness of non-context-freeness.

All that remains to complete the proof of the lemma is to establish that $(v_1, \tau_1, \ldots, v_h, \tau_h)$ is a self-covering sequence. First, observe that, by construction, $\mathsf{Sup}(V) \cup \{h\} = \{1, \ldots, h\}$. Let $t \in \{1, \ldots, h\}$ such that $\Delta(\tau_t) \not\geq \boldsymbol{0}$. There are two cases to consider.

- If $t < h$ then $t \in \mathsf{Sup}(V)$. Since $\Delta(\tau_t) \not\geq \mathbf{0}$, we get that $(s,t) \in V$ for some $s \in \{1,\ldots,h\}$. It follows that $\|\Delta(\tau_t)\|^- \subseteq \|\Delta(\tau_r)\|^+$ for some $(r,t) \in V$. Hence, $\|\Delta(\tau_t)\|^- \subseteq \bigcup_{j=1}^{t-1} \|\Delta(\tau_j)\|^+$.
- If $t = h$ then $\|\Delta(\tau_t)\|^- = \|\Delta(\tau_h)\|^- \subseteq \|\mathsf{exc}(\tau_1,\ldots,\tau_h,V)\|^+$. Moreover, it is readily seen that $\|\mathsf{exc}(\tau_1,\ldots,\tau_h,V)\|^+ \subseteq \bigcup_{j=1}^{h} \|\Delta(\tau_j)\|^+$. We derive that $\|\Delta(\tau_t)\|^- \subseteq \bigcup_{j=1}^{t-1} \|\Delta(\tau_j)\|^+$.

We have shown that $(v_1,\tau_1,\ldots,v_h,\tau_h)$ is a self-covering sequence, which concludes the proof of the lemma. $\qquad\square$

Lemma E.2. *Every non-empty irreflexive nested relation R on $\{1,\ldots,k\}$ contains a pair $(\hat{s},\hat{t})$ such that*

$$\{s \mid (s,\hat{t}) \in R\} = \{\hat{s}\} \qquad or \qquad \{t \mid (\hat{s},t) \in R\} = \{\hat{t}\}$$

Proof. Consider a non-empty binary relation R on $\{1,\ldots,k\}$ that is both irreflexive (i.e., $s \neq t$ for every $(s,t) \in R$) and nested (i.e., R satisfies (1) and (2)). By contradiction, assume that the lemma condition does not hold. This means that for every pair $(s,t) \in R$, there exists $s' \neq s$ and $t' \neq t$ such that $(s',t) \in R$ and $(s,t') \in R$. Since $R \neq \emptyset$, we obtain that there exists in R two distinct pairs with the same target. Recall that R satisfies (1) and is irreflexive. We derive that there exists $s_0 < s_1 < t_0$ such that $(s_0,t_0) \in R$ and $(s_1,t_0) \in R$. Since $(s_1,t_0) \in R$, we obtain that there exists $t_1 \neq t_0$ such that $(s_1,t_1) \in R$. Observe that $s_1 < t_1$ as R satisfies (1) and is irreflexive. Furthermore, it holds that $t_1 < t_0$ as R satisfies (2). Let us replay this construction. Since $(s_1,t_1) \in R$, we obtain that there exists $s_2 \neq s_1$ such that $(s_2,t_1) \in R$. Moreover, it holds that $s_1 < s_2 < t_1$ as R satisfies (1) and (2) and is irreflexive. By iterating this process ad infinitum, we obtain that there exists two infinite sequences $(s_i)_{i \in \mathbb{N}}$ and $(t_i)_{i \in \mathbb{N}}$ such that $0 \leq s_0 < s_1 < \cdots < s_i < \cdots < t_i < \cdots < t_1 < t_0 \leq k$, which is obviously impossible. $\qquad\square$

Lemma E.3. *For every $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{Z}^d$ and $n_1, n_2 \in \mathbb{N}$, with $n_2 \neq 0$, it holds that*

$$\mathsf{rat}(n_1\boldsymbol{v}_1, n_2\boldsymbol{v}_2) = \frac{n_1}{n_2} \cdot \mathsf{rat}(\boldsymbol{v}_1, \boldsymbol{v}_2)$$
$$\mathsf{exc}(n_1\boldsymbol{v}_1, n_2\boldsymbol{v}_2) = n_1 \cdot \mathsf{exc}(\boldsymbol{v}_1, \boldsymbol{v}_2)$$

Proof. These two equalities are easily derived from the definitions. $\qquad\square$

Lemma E.4. *For every matching scheme $(\sigma_1,\ldots,\sigma_k,U)$, there exists k natural numbers $n_1,\ldots,n_k \in \mathbb{N}$, with $n_i > 0$, such that*

$$\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \left\{0, \frac{n_t}{n_s}\right\}$$

for every $(s,t) \in U$.

Proof. By induction on the cardinal of U. The basis, where $U = \emptyset$, is trivial. Consider a matching scheme $(\sigma_1, \ldots, \sigma_k, U)$ with $U \neq \emptyset$. Note that, by definition, U is a nested binary relation on $\{1, \ldots, k\}$. Moreover, U is irreflexive since every pair $(s, t) \in U$ verifies $\Delta(\sigma_s) \geq \mathbf{0}$ and $\Delta(\sigma_t) \not\geq \mathbf{0}$. According to Lemma E.2, there exists a pair $(\hat{s}, \hat{t}) \in U$ such that:

$$\{s \mid (s, \hat{t}) \in U\} = \{\hat{s}\} \quad \text{or} \quad \{t \mid (\hat{s}, t) \in U\} = \{\hat{t}\}$$

Let $V = U \setminus \{(\hat{s}, \hat{t})\}$. Obviously, $(\sigma_1, \ldots, \sigma_k, V)$ is also a matching scheme. It follows from the induction hypothesis that there exists $n_1, \ldots, n_k \in \mathbb{N}$, with $n_i > 0$, such that $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \{0, \frac{n_t}{n_s}\}$ for every $(s, t) \in V$. Recall that the ratio of any matching pair is a non-negative rational number. Let us write $\mathsf{rat}(\Delta(\sigma_{\hat{s}}), \Delta(\sigma_{\hat{t}})) = \frac{p}{q}$ where $p, q \in \mathbb{N}$, with $q \neq 0$. If $p = 0$ then we get that $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \{0, \frac{n_t}{n_s}\}$ for every $(s, t) \in U$, and so we are done. Otherwise, $p > 0$, and we define $m_1, \ldots, m_k \in \mathbb{N}$ as follows:

$$\text{If} \quad \{s \mid (s, \hat{t}) \in U\} = \{\hat{s}\} \quad \text{then} \quad m_i = \begin{cases} n_i \cdot p \cdot n_{\hat{s}} & \text{if } i = \hat{t} \\ n_i \cdot q \cdot n_{\hat{t}} & \text{if } i \neq \hat{t} \end{cases}$$

$$\text{If} \quad \{t \mid (\hat{s}, t) \in U\} = \{\hat{t}\} \quad \text{then} \quad m_i = \begin{cases} n_i \cdot q \cdot n_{\hat{t}} & \text{if } i = \hat{s} \\ n_i \cdot p \cdot n_{\hat{s}} & \text{if } i \neq \hat{s} \end{cases}$$

Observe that $m_i > 0$ for all $i \in \{1, \ldots, k\}$. To conclude the proof of the lemma, it remains to show that every $(s, t) \in U$ verifies $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \left\{0, \frac{m_t}{m_s}\right\}$. Let $(s, t) \in U$. If $(s, t) = (\hat{s}, \hat{t})$ then, by definition, $\frac{m_t}{m_s} = \frac{p}{q} = \mathsf{rat}(\Delta(\sigma_{\hat{s}}), \Delta(\sigma_{\hat{t}}))$. Otherwise, it holds that $(s, t) \in V$, which entails that $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \{0, \frac{n_t}{n_s}\}$. Let us show that $\frac{m_t}{m_s} = \frac{n_t}{n_s}$. There are two cases to consider.

- If $\{s \mid (s, \hat{t}) \in U\} = \{\hat{s}\}$ then $t \neq \hat{t}$ since $(s, t) \neq (\hat{s}, \hat{t})$. Moreover, $s \neq \hat{t}$ since $\Delta(\sigma_s) \geq \mathbf{0}$ and $\Delta(\sigma_{\hat{t}}) \not\geq \mathbf{0}$. It follows that $m_s = n_s \cdot q \cdot n_{\hat{t}}$ and $m_t = n_t \cdot q \cdot n_{\hat{t}}$.
- If $\{t \mid (\hat{s}, t) \in U\} = \{\hat{t}\}$ then $s \neq \hat{s}$ since $(s, t) \neq (\hat{s}, \hat{t})$. Moreover, $t \neq \hat{s}$ since $\Delta(\sigma_t) \not\geq \mathbf{0}$ and $\Delta(\sigma_{\hat{s}}) \geq \mathbf{0}$. It follows that $m_s = n_s \cdot p \cdot n_{\hat{s}}$ and $m_t = n_t \cdot p \cdot n_{\hat{s}}$.

In both cases, we obtain that $\frac{m_t}{m_s} = \frac{n_t}{n_s}$. Therefore, $\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \{0, \frac{m_t}{m_s}\}$ for every pair $(s, t) \in U$. $\qquad\square$

Proposition 8.3. *The trace language of a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ is not context-free if, and only if, $\langle \boldsymbol{A}, \boldsymbol{c}_{init} \rangle$ admits a perfect witness of non-context-freeness.*

Proof. The "if" direction follows from Theorem 8.2. For the converse, assume that the trace language of $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ is not context-free. According to Theorem 8.2 and Lemma E.1, $\langle \boldsymbol{A}, \boldsymbol{c}_{\text{init}} \rangle$ admits a witness of non-context-freeness $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$ such that $k \leq 3d + 1$ and $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ is a self-covering sequence. Since $(\sigma_1, \ldots, \sigma_k, U)$ is a matching scheme, we obtain from Lemma E.4 that there exists k natural numbers $n_1, \ldots, n_k \in \mathbb{N}$, with $n_i > 0$, such that

$$\mathsf{rat}(\Delta(\sigma_s), \Delta(\sigma_t)) \in \left\{0, \frac{n_t}{n_s}\right\} \tag{7}$$

for every $(s,t) \in U$. By Lemma 2.2, there exists $m_1, \ldots, m_k \geq \max\{n_1, \ldots, n_k\}$ such that $u_1\sigma_1^{m_1} \cdots u_k\sigma_k^{m_k}$ is a trace. Define $v_i = u_i\sigma_i^{m_i - n_i}$ for all $i \in \{1, \ldots, k\}$. since it is equal to $u_1\sigma_1^{m_1} \cdots u_k\sigma_k^{m_k}$. We show that $(v_1, \sigma_1^{n_1}, \ldots, v_k, \sigma_k^{n_k}, U)$ is a perfect witness of non-context-freeness. First, observe that

$$\|\Delta(\sigma_j^{n_j})\|^- = \|\Delta(\sigma_j)\|^- \quad \text{and} \quad \|\Delta(\sigma_j^{n_j})\|^+ = \|\Delta(\sigma_j)\|^+ \quad (8)$$

for all $j \in \{1, \ldots, k\}$. Since $(\sigma_1, \ldots, \sigma_k, U)$ is a matching scheme, we derive from (8) that $(\sigma_1^{n_1}, \ldots, \sigma_k^{n_k}, U)$ is a also matching scheme. Let us prove that $(v_1, \sigma_1^{n_1}, \ldots, v_k, \sigma_k^{n_k}, U)$ fulfills the three conditions of Definition 8.1. Recall that these conditions are satisfied by $(u_1, \sigma_1, \ldots, u_k, \sigma_k, U)$.

1. The word $v_1\sigma_1^{n_1} \cdots v_k\sigma_k^{n_k}$ is a trace since it is equal to $u_1\sigma_1^{m_1} \cdots u_k\sigma_k^{m_k}$, which is a trace.
2. It holds that $\|\Delta(\sigma_k^{n_k})\|^- = \|\Delta(\sigma_k)\|^- \neq \emptyset$. Moreover, Lemma E.3 entails that $\mathsf{exc}(\sigma_1^{n_1}, \ldots, \sigma_k^{n_k}, U) \geq \mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)$. Hence, $\|\Delta(\sigma_k^{n_k})\|^- = \|\Delta(\sigma_k)\|^- \subseteq \|\mathsf{exc}(\sigma_1, \ldots, \sigma_k, U)\|^+ \subseteq \|\mathsf{exc}(\sigma_1^{n_1}, \ldots, \sigma_k^{n_k}, U)\|^+$.
3. For every $(s,t) \in U$ with $t < k$, there exists $(r,t) \in U$ such that $r \leq s$ and $\|\Delta(\sigma_t^{n_t})\|^- = \|\Delta(\sigma_t)\|^- \subseteq \|\Delta(\sigma_r)\|^+ = \|\Delta(\sigma_r^{n_r})\|^+$.

It remains to show that $(v_1, \sigma_1^{n_1}, \ldots, v_k, \sigma_k^{n_k}, U)$ is perfect. Recall that $k \leq 3d+1$ and that $(u_1, \sigma_1, \ldots, u_k, \sigma_k)$ is a self-covering sequence. Since $v_1\sigma_1^{n_1} \cdots v_k\sigma_k^{n_k}$ is a trace, we deduce from (8) that $(v_1, \sigma_1, \ldots, v_k, \sigma_k)$ is also a self-covering sequence. Moreover, we derive from (7) and Lemma E.3 that $\mathsf{rat}(\Delta(\sigma_s^{n_s}), \Delta(\sigma_t^{n_t})) \in \{0, 1\}$ for every $(s,t) \in U$. We have shown that $(v_1, \sigma_1^{n_1}, \ldots, v_k, \sigma_k^{n_k}, U)$ is a perfect witness of non-context-freeness, which concludes the proof of the proposition. $\qquad \square$

F Additional Material for Section 8

The formulas $\rho_0(s,t)$ and $\rho_1(s,t)$ specifying, respectively, that the matching pair $(\Delta(\sigma_s), \Delta(\sigma_t))$ has ratio 0 and 1, are defined below:

$$\rho_0(s,t) = \bigvee_{j=1}^{d} -\boldsymbol{\delta}_s(j) \geq 0 \ \wedge \ -\boldsymbol{\delta}_t(j) \geq 1$$

$$\rho_1(s,t) = \bigwedge_{j=1}^{d} \boldsymbol{\delta}_s(j) + \boldsymbol{\delta}_t(j) \geq 0 \ \wedge \ \bigvee_{j=1}^{d} (-\boldsymbol{\delta}_t(j) \geq 1 \ \wedge \ -\boldsymbol{\delta}_s(j) - \boldsymbol{\delta}_t(j) \geq 0)$$

Theorem 8.5. *The context-freeness problem for VAS is* ExpSpace-*complete.*

Proof. We have already proved ExpSpace-membership. For the exponential space lower bound, we show a reduction from the boundedness problem for VAS, which is known to be ExpSpace-hard [9]. Consider a VAS $\langle \boldsymbol{A}, \boldsymbol{c}_{\mathrm{init}} \rangle$ of dimension d. We construct the VAS $\langle \boldsymbol{A}', \boldsymbol{c}'_{\mathrm{init}} \rangle$ of dimension $d+3$ defined by

$$\boldsymbol{A}' = \{(\boldsymbol{a}, 0, 0, 0) \mid \boldsymbol{a} \in \boldsymbol{A}\} \cup \{-\boldsymbol{e}_i + \boldsymbol{e}_{d+1} \mid 1 \leq i \leq d\} \cup \{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3\}$$

$$\boldsymbol{c}'_{\mathrm{init}} = (\boldsymbol{c}_{\mathrm{init}}, 0, 0, 0)$$

26

where $\boldsymbol{b}_1 = -\boldsymbol{e}_{d+1} + \boldsymbol{e}_{d+2} + \boldsymbol{e}_{d+3}$, $\boldsymbol{b}_2 = -\boldsymbol{e}_{d+2}$ and $\boldsymbol{b}_3 = -\boldsymbol{e}_{d+3}$. Let us show that $\langle \boldsymbol{A}, \boldsymbol{c}_{\mathrm{init}} \rangle$ is bounded if, and only if, the trace language of $\langle \boldsymbol{A}', \boldsymbol{c}'_{\mathrm{init}} \rangle$ is context-free. If $\langle \boldsymbol{A}, \boldsymbol{c}_{\mathrm{init}} \rangle$ is bounded then $\langle \boldsymbol{A}', \boldsymbol{c}'_{\mathrm{init}} \rangle$ is also bounded, hence, its trace language is regular. Otherwise, $\langle \boldsymbol{A}, \boldsymbol{c}_{\mathrm{init}} \rangle$ is not bounded, and it follows, by construction, that the component at index $d+1$ can be arbitrarily large in $\boldsymbol{A}'$, through traces that do not use $\boldsymbol{b}_1$, $\boldsymbol{b}_2$ nor $\boldsymbol{b}_3$. Consider the language

$$L \;=\; \mathcal{T}(\boldsymbol{A}', \boldsymbol{c}'_{\mathrm{init}}) \,\cap\, ((\boldsymbol{A}' \setminus \{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3\})^* \cdot \boldsymbol{b}_1^* \cdot \boldsymbol{b}_2^* \cdot \boldsymbol{b}_3^*)$$

Its projection on $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3\}$ is the language $\{\boldsymbol{b}_1^{n_1} \boldsymbol{b}_2^{n_2} \boldsymbol{b}_3^{n_3} \mid n_1 \geq n_2 \wedge n_1 \geq n_3\}$, which is not context-free. Recall that the class of context-free languages is closed under projection and under intersection with regular languages. It follows that $\mathcal{T}(\boldsymbol{A}', \boldsymbol{c}'_{\mathrm{init}})$ is not context-free, which concludes the proof of ExpSpace-hardness. $\square$