

## AFFINE EXTENSIONS OF INTEGER VECTOR ADDITION SYSTEMS WITH STATES

MICHAEL BLONDIN, CHRISTOPH HAASE, FILIP MAZOWIECKI, AND MIKHAIL RASKIN

Université de Sherbrooke, Canada  
*e-mail address:* michael.blondin@usherbrooke.ca

University of Oxford, United Kingdom  
*e-mail address:* christoph.haase@cs.ox.ac.uk

Max Planck Institute for Software Systems, Germany  
*e-mail address:* filipm@mpi-sws.org

Technische Universität München, Germany  
*e-mail address:* raskin@in.tum.de

**ABSTRACT.** We study the reachability problem for affine  $\mathbb{Z}$ -VASS, which are integer vector addition systems with states in which transitions perform affine transformations on the counters. This problem is easily seen to be undecidable in general, and we therefore restrict ourselves to affine  $\mathbb{Z}$ -VASS with the finite-monoid property (afmp- $\mathbb{Z}$ -VASS). The latter have the property that the monoid generated by the matrices appearing in their affine transformations is finite. The class of afmp- $\mathbb{Z}$ -VASS encompasses classical operations of counter machines such as resets, permutations, transfers and copies. We show that reachability in an afmp- $\mathbb{Z}$ -VASS reduces to reachability in a  $\mathbb{Z}$ -VASS whose control-states grow linearly in the size of the matrix monoid. Our construction shows that reachability relations of afmp- $\mathbb{Z}$ -VASS are semilinear, and in particular enables us to show that reachability in  $\mathbb{Z}$ -VASS with transfers and  $\mathbb{Z}$ -VASS with copies is PSPACE-complete. We then focus on the reachability problem for affine  $\mathbb{Z}$ -VASS with monogenic monoids: (possibly infinite) matrix monoids generated by a single matrix. We show that, in a particular case, the reachability problem is decidable for this class, disproving a conjecture about affine  $\mathbb{Z}$ -VASS with infinite matrix monoids we raised in a preliminary version of this paper. We complement this result by presenting an affine  $\mathbb{Z}$ -VASS with monogenic matrix monoid and undecidable reachability relation.

---

\* A preliminary version of this paper appeared in the proceedings of the 29<sup>th</sup> International Conference on Concurrency Theory (CONCUR), 2018 [BHM18].

M. Blondin was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC), and by a Quebec-Bavaria project and a start-up grant funded by the Fonds de recherche du Québec – Nature et technologies (FRQNT).

F. Mazowiecki’s research has been carried out with financial support from the French State, managed by the French National Research Agency (ANR) in the frame of the “Investments for the future” Programme IdEx Bordeaux (ANR-10-IDEX-03-02).

M. Raskin was supported by funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme under grant agreement No 787367 (PaVeS).

## 1. INTRODUCTION

*Vector addition systems with states (VASS)* are a fundamental model of computation comprising a finite-state controller with a finite number of counters ranging over the natural numbers. When a transition is taken, a counter can be incremented or decremented provided that the resulting counter value is greater than or equal to zero. Since the counters of a VASS are unbounded, a VASS gives rise to an infinite transition system. One of the biggest advantages of VASS is that most of the standard decision problems such as configuration reachability and coverability are decidable [KM69, May84, Kos82, Ler12]. Those properties make VASS and their extensions a prime choice for reasoning about and modelling concurrent, distributed and parametrised systems, see *e.g.* the recent surveys by Abdulla and Delzanno [AD16, Del16].

In order to increase their modelling power, numerous extensions of plain VASS have been proposed and studied in the literature over the last 25 years. Due to the infinite-state nature of VASS, even minor extensions often cross the undecidability frontier. For example, while in the extension of VASS with hierarchical zero-tests on counters both reachability and coverability remain decidable [Rei08, Bon13], all important decision problems for VASS with two counters which can arbitrarily be tested for zero are undecidable [Min67]. Another example is the extension of VASS with reset and transfer operations. In a *reset VASS*, transitions may set a counter to zero, whereas *transfer VASS* generalize reset VASS and allow transitions to move the contents of a counter onto another. While it was initially widely believed that any extension of VASS either renders both reachability and coverability undecidable, reset and transfer VASS have provided an example of an extension which leads to an undecidable reachability [AK76] yet decidable coverability problem [DFPS98]. Nevertheless, the computational costs for those extensions are high: while coverability is EXPSPACE-complete for VASS [Lip76, Rac78], it becomes Ackermann-complete in the presence of resets and transfers [Sch10, FFSPS11]. For practical purposes, the extension of VASS with transfers is particularly useful since transfer VASS allow for reasoning about broadcast protocols and multithreaded non-recursive C programs [EN98, KKW14]. It was already observed in [EN98] that transfer VASS can be viewed as an instance of so-called *affine VASS*. An affine VASS is a generalization of VASS with transitions labelled by pairs  $(\mathbf{A}, \mathbf{b})$ , where  $\mathbf{A}$  is a  $d \times d$  matrix over the integers and  $\mathbf{b} \in \mathbb{Z}^d$  is an integer vector. A transition switches the control-state while updating the configuration of the counters  $\mathbf{v} \in \mathbb{N}^d$  to  $\mathbf{A} \cdot \mathbf{v} + \mathbf{b}$ , provided that  $\mathbf{A} \cdot \mathbf{v} + \mathbf{b} \geq \mathbf{0}$ ; otherwise, the transition is blocked. Transfer VASS can be viewed as affine VASS in which the columns of all matrices are  $d$ -dimensional unit vectors [EN98].

Due to the symbolic state-explosion problem and Ackermann-hardness of coverability, standard decision procedures for transfer VASS such as the backward algorithm [ACJT96] do not *per se* scale to real-world instances. In recent years, numerous authors have proposed the use of over-approximations in order to attenuate the symbolic state-explosion problem for VASS and some of their extensions (see, *e.g.*, [ELM<sup>+</sup>14, ALW16, BH17]). Most commonly, the basic idea is to relax the integrality or non-negativity condition on the counters and to allow them to take values from the non-negative rational numbers or the integers. The latter class is usually referred to as  $\mathbb{Z}$ -VASS, see *e.g.* [HH14]. It is easily seen that if a configuration is not reachable under the relaxed semantics, then the configuration is also not reachable under the standard semantics. Hence, those state-space over-approximations can, for instance, be used to prune search spaces and empirically drastically speedup classical algorithms for

VASS such as the backward-algorithm. In this paper, we investigate reachability in *integer over-approximations* of affine VASS, *i.e.*, affine VASS in which a configuration of the counters is a point in  $\mathbb{Z}^d$ , and in which all transitions are non-blocking. Subsequently, we refer to such VASS as *affine  $\mathbb{Z}$ -VASS*.

**Main contributions.** We focus on affine  $\mathbb{Z}$ -VASS with the *finite-monoid property* (afmp- $\mathbb{Z}$ -VASS), *i.e.* where the matrix monoid generated by all matrices occurring along transitions in the affine  $\mathbb{Z}$ -VASS is finite. By a reduction to reachability in  $\mathbb{Z}$ -VASS, we obtain decidability of reachability for the whole class of afmp- $\mathbb{Z}$ -VASS and semilinearity of their reachability relations.

In more detail, we show that reachability in an afmp- $\mathbb{Z}$ -VASS can be reduced to reachability in a  $\mathbb{Z}$ -VASS whose size is polynomial in the size of the original afmp- $\mathbb{Z}$ -VASS and in the norm of the finite monoid  $\mathcal{M}$  generated by the matrices occurring along transitions, denoted by  $\|\mathcal{M}\|$ . For a vast number of classes of affine transformations considered in the literature,  $\|\mathcal{M}\|$  is bounded exponentially in the dimension of the matrices. This enables us to deduce a general PSPACE upper bound for extensions of  $\mathbb{Z}$ -VASS such as transfer  $\mathbb{Z}$ -VASS and copy  $\mathbb{Z}$ -VASS. By a slightly more elaborated analysis of this construction, we are also able to provide a short proof of the already known NP upper bound for reset  $\mathbb{Z}$ -VASS [HH14]. We also show that a PSPACE lower bound of the reachability problem already holds for the extension of  $\mathbb{Z}$ -VASS that only use permutation matrices in their transition updates. This in turn gives PSPACE-completeness of interesting classes such as transfer  $\mathbb{Z}$ -VASS and copy  $\mathbb{Z}$ -VASS.

Finally, we show that an affine  $\mathbb{Z}$ -VASS that has both transfers and copies may not have the finite-monoid property, and that the reachability problem for this class becomes undecidable. We complement this result by investigating the case of monogenic classes, *i.e.* classes of monoids with a single generator. We show that although reachability can still be undecidable for an affine  $\mathbb{Z}$ -VASS with a monogenic matrix monoid, there exists a monogenic class without the finite-monoid property for which reachability is decidable.

All complexity results obtained in this paper are summarized in Figure 1, except for the undecidability of general monogenic classes as it is a family of classes rather than one class.

**Related work.** Our work is primarily related to the work of Finkel and Leroux [FL02], Iosif and Sangnier [IS16], Haase and Halfon [HH14], and Cadilhac, Finkel and McKenzie [CFM12, CFM13]. In [FL02], Finkel and Leroux consider a model more general than affine  $\mathbb{Z}$ -VASS in which transitions are additionally equipped with guards which are Presburger formulas defining admissible sets of vectors in which a transition does not block. Given a sequence of transitions  $\sigma$ , Finkel and Leroux show that the reachability set obtained from repeatedly iterating  $\sigma$ , *i.e.*, the *acceleration* of  $\sigma$ , is definable in Presburger arithmetic. Note that the model of Finkel and Leroux does not allow for control-states and the usual tricks of encoding each control-state by a counter or all control-states into three counters [HP79] do not work over  $\mathbb{Z}$  since transitions are non-blocking. Iosif and Sangnier [IS16] investigated the complexity of model checking problems for a variant of the model of Finkel and Leroux with guards defined by convex polyhedra and with control-states over a flat structure. Haase and Halfon [HH14] studied the complexity of the reachability, coverability and inclusion problems for  $\mathbb{Z}$ -VASS and reset  $\mathbb{Z}$ -VASS, two submodels of the affine  $\mathbb{Z}$ -VASS that we study in this paper. In [CFM12, CFM13], Cadilhac, Finkel and McKenzie consider an extension of Parikh automata to affine Parikh automata with the finite-monoid restriction like in our paper. These are automata recognizing boolean languages, but the finite-monoid restriction

was exploited in a similar way to obtain some decidability results in that context. We finally remark that our models capture variants of cost register automata that have only one  $+$  operation [AR13, AFR14].

**Structure of the paper.** We introduce general notations and affine  $\mathbb{Z}$ -VASS in Section 2. In Section 3, we give the reduction from afmp- $\mathbb{Z}$ -VASS to  $\mathbb{Z}$ -VASS. Subsequently, in Section 4 we show that afmp- $\mathbb{Z}$ -VASS have semilinear reachability relations and discuss semilinearity of affine  $\mathbb{Z}$ -VASS in general. In Section 5, we show PSPACE and NP upper bounds of the reachability problem for some classes of afmp- $\mathbb{Z}$ -VASS; and in Section 6 we show PSPACE-hardness and undecidability results for some classes of affine  $\mathbb{Z}$ -VASS. In Section 7, we show that reachability is undecidable for monogenic affine  $\mathbb{Z}$ -VASS and remains decidable for a specific class of infinite monoids. Some concluding remarks will be made in Section 8.

## 2. PRELIMINARIES

**General notation.** For  $n \in \mathbb{N}$ , we write  $[n]$  for the set  $\{1, 2, \dots, n\}$ . For every  $\mathbf{x} = (x_1, x_2, \dots, x_d) \in \mathbb{Z}^d$  and every  $i \in [d]$ , we define  $\mathbf{x}(i) \stackrel{\text{def}}{=} x_i$ . We denote the identity matrix and the zero-vector by  $\mathbf{I}$  and  $\mathbf{0}$  in every dimension, as there will be no ambiguity. For  $\mathbf{x} \in \mathbb{Z}^d$  and  $\mathbf{A} \in \mathbb{Z}^{d \times d}$ , we define the *max-norm* of  $\mathbf{x}$  and  $\mathbf{A}$  as  $\|\mathbf{x}\| \stackrel{\text{def}}{=} \max\{|\mathbf{x}(i)| : i \in [d]\}$  and  $\|\mathbf{A}\| \stackrel{\text{def}}{=} \max\{\|\mathbf{A}_i\| : i \in [d]\}$  where  $\mathbf{A}_i$  denotes the  $i^{\text{th}}$  column of  $\mathbf{A}$ . We naturally extend this notation to finite sets, *i.e.*  $\|G\| \stackrel{\text{def}}{=} \max\{\|\mathbf{A}\| : \mathbf{A} \in G\}$  for every  $G \subseteq_{\text{fin}} \mathbb{Z}^{d \times d}$ . We assume that numbers are represented in binary, hence the entries of vectors and matrices can be exponential in the size of their encodings.

**Affine Integer VASS.** An *affine integer vector addition system with states* (affine  $\mathbb{Z}$ -VASS) is a tuple  $\mathcal{V} = (d, Q, T)$  where  $d \in \mathbb{N}$ ,  $Q$  is a finite set and  $T \subseteq Q \times \mathbb{Z}^{d \times d} \times \mathbb{Z}^d \times Q$  is finite. Let us fix such a  $\mathcal{V}$ . We call  $d$  the *dimension* of  $\mathcal{V}$  and the elements of  $Q$  and  $T$  respectively *control-states* and *transitions*. For every transition  $t = (p, \mathbf{A}, \mathbf{b}, q)$ , we define  $\text{src}(t) \stackrel{\text{def}}{=} p$ ,  $\text{tgt}(t) \stackrel{\text{def}}{=} q$ ,  $M(t) \stackrel{\text{def}}{=} \mathbf{A}$  and  $\Delta(t) \stackrel{\text{def}}{=} \mathbf{b}$ , and let  $f_t: \mathbb{Z}^d \rightarrow \mathbb{Z}^d$  be the affine transformation defined by  $f_t(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} + \mathbf{b}$ . The *size* of  $\mathcal{V}$ , denoted  $|\mathcal{V}|$ , is the number of bits used to represent  $d$ ,  $Q$  and  $T$  with coefficients written in binary. For our purposes, we formally define it in a crude way as  $|\mathcal{V}| \stackrel{\text{def}}{=} d + |Q| + (d^2 + d) \cdot |T| \cdot \max(1, \lceil \log(\|T\| + 1) \rceil)$  where

$$\|T\| \stackrel{\text{def}}{=} \max(\max\{\|\Delta(t)\| : t \in T\}, \max\{\|M(t)\| : t \in T\}).$$

A *configuration* of  $\mathcal{V}$  is a pair  $(q, \mathbf{v}) \in Q \times \mathbb{Z}^d$  which we write as  $q(\mathbf{v})$ . For every  $t \in T$  and  $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{Z}^d$ , we write  $p(\mathbf{u}) \xrightarrow{t} q(\mathbf{v})$  whenever  $p = \text{src}(t)$ ,  $q = \text{tgt}(t)$  and  $\mathbf{v} = f_t(\mathbf{u})$ . We naturally extend  $\rightarrow$  to sequences of transitions as follows. For every  $w = w_1 \cdots w_k \in T^k$  and  $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{Z}^d$ , we write  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$  if either  $k = 0$  (denoted  $w = \varepsilon$ ) and  $p(\mathbf{u}) = q(\mathbf{v})$ , or  $k > 0$  and there exist  $p_0(\mathbf{u}_0), p_1(\mathbf{u}_1), \dots, p_k(\mathbf{u}_k) \in Q \times \mathbb{Z}^d$  such that

$$p(\mathbf{u}) = p_0(\mathbf{u}_0) \xrightarrow{w_1} p_1(\mathbf{u}_1) \xrightarrow{w_2} \cdots \xrightarrow{w_k} p_k(\mathbf{u}_k) = q(\mathbf{v}).$$

We write  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$  if there exists some  $w \in T^*$  such that  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$ . The relation  $\xrightarrow{*}$  is called the *reachability relation* of  $\mathcal{V}$ . If  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$ , then we say that  $w$  is a *run from  $p(\mathbf{u})$  to  $q(\mathbf{v})$* , or simply a *run* if the source and target configurations are irrelevant. We also say that  $w$  is a *path* from  $p$  to  $q$ , and if  $p = q$  then we say that  $w$  is a *cycle*.

Let  $M(\mathcal{V}) \stackrel{\text{def}}{=} \{M(t) : t \in T\}$  and  $\Delta(\mathcal{V}) \stackrel{\text{def}}{=} \{\Delta(t) : t \in T\}$ . If  $\mathcal{V}$  is clear from the context, we sometimes simply write  $M$  and  $\Delta$ . The *monoid of  $\mathcal{V}$* , denoted  $\mathcal{M}_{\mathcal{V}}$  or sometimes simply

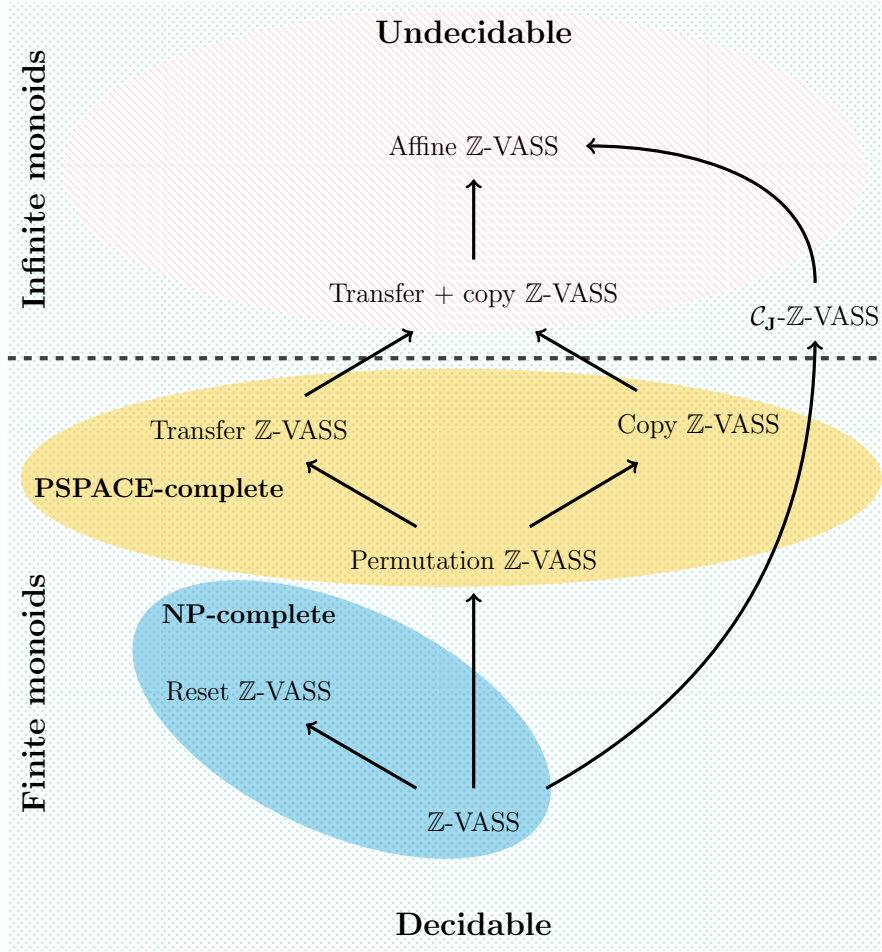


FIGURE 1. Classification of the complexity of reachability in affine  $\mathbb{Z}$ -VASS in terms of classes of matrices. The rectangular regions below and above the horizontal dashed line correspond to classes of matrices with finite and infinite monoids respectively. The rectangular green dotted region and the elliptical red striped region correspond to the classes where reachability is decidable and undecidable, respectively. The elliptical blue region and the orange elliptical region correspond to the classes where reachability is NP-complete and PSPACE-complete respectively. The term “ $\mathcal{C}_J$ - $\mathbb{Z}$ -VASS” refers to the specific monogenic class of infinite monoids that will be defined in Section 7.1.

$\mathcal{M}$ , is the monoid generated by  $M(\mathcal{V})$ , *i.e.* it is the smallest set that contains  $M(\mathcal{V})$ , is closed under matrix multiplication, and contains the identity matrix. We say that a matrix  $\mathbf{A} \in \mathbb{N}^{d \times d}$  is respectively a (i) *reset*, (ii) *permutation*, (iii) *transfer*, (iv) *copyless*, or (v) *copy* matrix if  $\mathbf{A} \in \{0, 1\}^{d \times d}$  and

- (i)  $\mathbf{A}$  does not contain any 1 outside of its diagonal;
- (ii)  $\mathbf{A}$  has exactly one 1 in each row and each column;
- (iii)  $\mathbf{A}$  has exactly one 1 in each column;
- (iv)  $\mathbf{A}$  has at most one 1 in each column;

(v)  $\mathbf{A}$  has exactly one 1 in each row.

Analogously, we say that  $\mathcal{V}$  is respectively a *reset*, *permutation*, *transfer*, *copyless*, or *copy*  $\mathbb{Z}$ -VASS if all matrices of  $M(\mathcal{V})$  are reset, permutation, transfer, copyless, or copy matrices. The monoids of such affine  $\mathbb{Z}$ -VASS are finite and respectively of size at most  $2^d$ ,  $d!$ ,  $d^d$ ,  $(d+1)^d$  and  $d^d$ . Copyless  $\mathbb{Z}$ -VASS correspond to a model of copyless cost-register automata studied in [AFR14] (see the remark below). If  $M(\mathcal{V})$  only contains the identity matrix, then  $\mathcal{V}$  is simply called a  $\mathbb{Z}$ -VASS.

A *class of matrices*  $\mathcal{C}$  is a union  $\bigcup_{d \geq 1} \mathcal{C}_d$  where  $\mathcal{C}_d$  is a finitely generated, but possibly infinite, submonoid of  $\mathbb{N}^{d \times d}$  for every  $d \geq 1$ . We say that  $\mathcal{V}$  belongs to a class  $\mathcal{C}$  of  $\mathbb{Z}$ -VASS if  $\mathcal{M}_{\mathcal{V}} \subseteq \mathcal{C}$ . If each  $\mathcal{C}_d$  is finite, then we say that this class of affine  $\mathbb{Z}$ -VASS has the *finite-monoid property* (afmp- $\mathbb{Z}$ -VASS). For two classes  $\mathcal{C}$  and  $\mathcal{C}'$  we write  $\mathcal{C} + \mathcal{C}'$  to denote the smallest set  $\mathcal{D} = \bigcup_{d \geq 1} \mathcal{D}_d$  such that  $\mathcal{D}_d$  is a monoid that contains both  $\mathcal{C}_d$  and  $\mathcal{C}'_d$  for every  $d \geq 1$ . Note that this operation does not preserve finiteness. For example if  $\mathcal{C}$  and  $\mathcal{C}'$  are the classes of transfer and copy matrices, respectively, then  $\mathcal{C} + \mathcal{C}'$  is infinite (see Figure 2 and Section 6). We say that a class  $\mathcal{C} = \bigcup_{d \geq 1} \mathcal{C}_d$  is *nonnegative* if  $\mathcal{C}_d \subseteq \mathbb{N}^{d \times d}$  for every  $d \geq 1$ . We say that an affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$  is *nonnegative* if  $\mathcal{M}_{\mathcal{V}}$  belongs to some nonnegative class of matrices. Note that the classes of reset, permutation, transfer, copyless and copy matrices are all nonnegative, respectively.

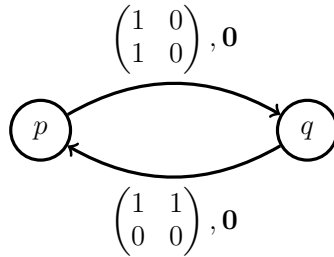


FIGURE 2. Example of a transfer + copy  $\mathbb{Z}$ -VASS  $\mathcal{V}$  which does not have the finite-monoid property.

We discuss the  $\mathbb{Z}$ -VASS  $\mathcal{V}$  in Figure 2 to give some intuition behind the names transfer and copy  $\mathbb{Z}$ -VASS. The transition from  $p$  to  $q$  is a copy transition and the transition from  $q$  to  $p$  is a transfer transition. Notice that for every vector  $(x, y) \in \mathbb{Z}^2$ , we have  $p(x, y) \rightarrow q(x, x)$ , *i.e.* the value of the first counter is copied to the second counter. Similarly, for the other transition we have  $q(x, y) \rightarrow p(x + y, 0)$ , that is the value of the second counter is transferred to the first counter (resetting its own value to 0). Let  $\mathbf{A}$  and  $\mathbf{B}$  be the two matrices used in  $\mathcal{V}$ . Note that  $(\mathbf{A} \cdot \mathbf{B})^n$  is the matrix with all entries equal to  $2^{n-1}$ , and hence  $\mathcal{M}_{\mathcal{V}}$  is infinite.

**Remark 2.1.** The variants of affine  $\mathbb{Z}$ -VASS that we consider are related to cost register automata (CRA) with only the  $+$  operation [AR13, AFR14] and without an output function. These are deterministic models with states and registers that upon reading an input, update their registers in the form  $x \leftarrow y + c$ , where  $x, y$  are registers and  $c$  is an integer. An affine  $\mathbb{Z}$ -VASS does not read any input, but is nondeterministic. Thus, one can identify an affine  $\mathbb{Z}$ -VASS with a CRA that reads sequences of transitions as words. In particular, the restrictions imposed on the studied CRAs correspond to copy  $\mathbb{Z}$ -VASS [AR13] and copyless  $\mathbb{Z}$ -VASS [AFR14].

**Decision problems.** We consider the *reachability* and the *coverability* problems parameterized by classes of matrices  $\mathcal{C}$ :

Reach $_{\mathcal{C}}$  (reachability problem)

GIVEN: an affine  $\mathbb{Z}$ -VASS  $\mathcal{V} = (d, Q, T)$  and configurations  $p(\mathbf{u}), q(\mathbf{v})$  s.t.  $\mathcal{M}_{\mathcal{V}} \subseteq \mathcal{C}$ .

DECIDE: whether  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$ .

Cover $_{\mathcal{C}}$  (coverability problem)

GIVEN: an affine  $\mathbb{Z}$ -VASS  $\mathcal{V} = (d, Q, T)$  and configurations  $p(\mathbf{u}), q(\mathbf{v})$  s.t.  $\mathcal{M}_{\mathcal{V}} \subseteq \mathcal{C}$ .

DECIDE: whether there exists  $\mathbf{v}' \in \mathbb{Z}^d$  such that  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v}')$  and  $\mathbf{v}' \geq \mathbf{v}$ .

For standard VASS (where configurations cannot hold negative values), the coverability problem is much simpler than the reachability problem. However, for affine  $\mathbb{Z}$ -VASS, these two problems coincide as observed in [HH14, Lemma 2]: the two problems are inter-reducible in logarithmic space at the cost of doubling the number of counters. Therefore we will only study the reachability problem in this paper.

### 3. FROM AFFINE $\mathbb{Z}$ -VASS WITH THE FINITE-MONOID PROPERTY TO $\mathbb{Z}$ -VASS

The main result of this section is that every affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$  with the finite monoid property can be simulated by a  $\mathbb{Z}$ -VASS with twice the number of counters whose size is polynomial in  $\|\mathcal{M}_{\mathcal{V}}\|$  and  $|\mathcal{V}|$ . More formally, we show the following:

**Theorem 3.1.** *For every afmp- $\mathbb{Z}$ -VASS  $\mathcal{V} = (d, Q, T)$  and  $p, q \in Q$  there exist a  $\mathbb{Z}$ -VASS  $\mathcal{V}' = (d', Q', T')$  and  $p', q' \in Q'$  such that*

- $d' = 2 \cdot d$ ,
- $|Q'| \leq 3 \cdot |\mathcal{M}_{\mathcal{V}}| \cdot |Q|$ ,
- $|T'| \leq 4d \cdot |\mathcal{M}_{\mathcal{V}}| \cdot (|Q| + |T|)$ ,
- $\|T'\| \leq \|\mathcal{M}_{\mathcal{V}}\| \cdot \|T\|$ ,
- $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$  in  $\mathcal{V}$  if and only if  $p'(\mathbf{u}, \mathbf{0}) \xrightarrow{*} q'(\mathbf{0}, \mathbf{v})$  in  $\mathcal{V}'$ .

Moreover,  $\mathcal{V}', p'$  and  $q'$  are effectively computable from  $\mathcal{V}$ .

**Corollary 3.2.** *The reachability problem for afmp- $\mathbb{Z}$ -VASS is decidable.*

*Proof.* By Theorem 3.1, it suffices to construct, for a given afmp- $\mathbb{Z}$ -VASS  $\mathcal{V}$ , the  $\mathbb{Z}$ -VASS  $\mathcal{V}'$  and to test for reachability in  $\mathcal{V}'$ . It is known that reachability for  $\mathbb{Z}$ -VASS is in NP [HH14]. To effectively compute  $\mathcal{V}'$  it suffices to provide a bound for  $\|\mathcal{M}_{\mathcal{V}}\|$ . It is known that if  $|\mathcal{M}_{\mathcal{V}}|$  is finite then it is bounded by a computable function (see [MS77]), and hence  $\|\mathcal{M}_{\mathcal{V}}\|$  is also computable.  $\square$

For the remainder of this section, let us fix some affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$  such that  $\mathcal{M}_{\mathcal{V}}$  is finite. We proceed as follows to prove Theorem 3.1. First, we introduce some notations and intermediary lemmas characterizing reachability in affine  $\mathbb{Z}$ -VASS. Next, we give a construction that essentially proves the special case of Theorem 3.1 where the initial configuration is of the form  $p(\mathbf{0})$ . Finally, we prove Theorem 3.1 by extending this construction to the general case.

It is worth noting that proving the general case is not necessary if one is only interested in deciding reachability. Indeed, an initial configuration  $p(\mathbf{v})$  can be turned into one of the

form  $p'(\mathbf{0})$  by adding a transition that adds  $\mathbf{v}$ . The reason for proving the general case is that it establishes a stronger relation that allows us to prove semilinearity of afmp- $\mathbb{Z}$ -VASS reachability relations in Section 4.

**3.1. A characterization of reachability.** For every  $w \in T^*$ ,  $t \in T$  and  $\mathbf{u} \in \mathbb{Z}^d$ , let

$$\begin{aligned} M(\varepsilon) &\stackrel{\text{def}}{=} \mathbf{I}, & \varepsilon(\mathbf{u}) &\stackrel{\text{def}}{=} \mathbf{u}, \\ M(wt) &\stackrel{\text{def}}{=} M(t) \cdot M(w), & wt(\mathbf{u}) &\stackrel{\text{def}}{=} M(t) \cdot w(\mathbf{u}) + \Delta(t). \end{aligned}$$

Intuitively, for any sequence  $w \in T^*$ ,  $w(\mathbf{u})$  is the effect of  $w$  on  $\mathbf{u}$ , regardless of whether  $w$  is an actual path of the underlying graph. A simple induction yields the following characterization:

**Lemma 3.3.** *For every  $w \in T^*$  and  $p(\mathbf{u}), q(\mathbf{v}) \in Q \times \mathbb{Z}^d$ , it is the case that  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$  if and only if*

- (a)  $w$  is a path from  $p$  to  $q$  in the underlying graph of  $\mathcal{V}$ , and
- (b)  $\mathbf{v} = w(\mathbf{u})$ .

Testing for reachability with Lemma 3.3 requires evaluating  $w(\mathbf{u})$ . This value can be evaluated conveniently as follows:

**Lemma 3.4.** *For every  $w = w_1 w_2 \cdots w_k \in T^k$  and  $\mathbf{u} \in \mathbb{Z}^d$ , the following holds:*

$$w(\mathbf{u}) = M(w) \cdot \mathbf{u} + \sum_{i=1}^k M(w_{i+1} w_{i+2} \cdots w_k) \cdot \Delta(w_i). \quad (3.1)$$

Moreover,  $w(\mathbf{u}) = M(w) \cdot \mathbf{u} + w(\mathbf{0})$ .

*Proof of Lemma 3.4.* We prove (3.1) by induction on  $k$ . The base case follows from  $\varepsilon(\mathbf{u}) = \mathbf{u} = \mathbf{I} \cdot \mathbf{u} + \mathbf{0} = M(\varepsilon) \cdot \mathbf{u} + \mathbf{0}$ . Assume that  $k > 0$  and that the claim holds for sequences of length  $k - 1$ . For simplicity we denote  $\sigma \stackrel{\text{def}}{=} w_1 \cdots w_{k-1}$ . We have:

$$\begin{aligned} w(\mathbf{u}) &= \sigma w_k(\mathbf{u}) \\ &= M(w_k) \cdot \sigma(\mathbf{u}) + \Delta(w_k) \end{aligned} \quad (3.2)$$

$$= M(w_k) \cdot \left( M(\sigma) \cdot \mathbf{u} + \sum_{i=1}^{k-1} M(w_{i+1} w_{i+2} \cdots w_{k-1}) \cdot \Delta(w_i) \right) + \Delta(w_k) \quad (3.3)$$

$$= M(w_k) \cdot M(\sigma) \cdot \mathbf{u} + \sum_{i=1}^{k-1} M(w_k) \cdot M(w_{i+1} w_{i+2} \cdots w_{k-1}) \cdot \Delta(w_i) + \Delta(w_k)$$

$$= M(\sigma w_k) \cdot \mathbf{u} + \sum_{i=1}^{k-1} M(w_{i+1} w_{i+2} \cdots w_k) \cdot \Delta(w_i) + \Delta(w_k) \quad (3.4)$$

$$= M(w) \cdot \mathbf{u} + \sum_{i=1}^k M(w_{i+1} w_{i+2} \cdots w_k) \cdot \Delta(w_i)$$

where (3.2), (3.3) and (3.4) follow respectively by definition of  $\sigma w_k(\mathbf{u})$ , by induction hypothesis and by definition of  $M(\sigma w_k)$ .

The last part of the lemma follows from applying (3.1) to  $w(\mathbf{0})$  and  $w(\mathbf{u})$ , and observing that subtracting them results in  $w(\mathbf{u}) - w(\mathbf{0}) = M(w) \cdot \mathbf{u}$ .  $\square$



Observe that Lemma 3.4 is trivial for the particular case of  $\mathbb{Z}$ -VASS. Indeed, we obtain  $w(\mathbf{u}) = \mathbf{u} + \sum_{i=1}^k \Delta(w_i)$ , which is the sum of transition vectors as expected for a  $\mathbb{Z}$ -VASS.

**3.2. Reachability from the origin.** We make use of Lemmas 3.3 and 3.4 to construct a  $\mathbb{Z}$ -VASS  $\mathcal{V}' = (d, Q', T')$  for the special case of Theorem 3.1 where the initial configuration is of the form  $p(\mathbf{0})$ . The states and transitions of  $\mathcal{V}'$  are defined as:

$$Q' \stackrel{\text{def}}{=} Q \times \mathcal{M},$$

$$T' \stackrel{\text{def}}{=} \{((\text{tgt}(t), \mathbf{A}), \mathbf{I}, \mathbf{A} \cdot \Delta(t), (\text{src}(t), \mathbf{A} \cdot M(t))) : \mathbf{A} \in \mathcal{M}, t \in T\}.$$

The idea behind  $\mathcal{V}'$  is to simulate a path  $w$  of  $\mathcal{V}$  backwards and to evaluate  $w(\mathbf{0})$  as the sum identified in Lemma 3.4. More formally,  $\mathcal{V}'$  and  $\mathcal{V}$  are related as follows:

**Proposition 3.5.**

- (a) For every  $w \in T^*$ , if  $p(\mathbf{0}) \xrightarrow{w} q(\mathbf{v})$  in  $\mathcal{V}$ , then  $q'(\mathbf{0}) \xrightarrow{*} p'(\mathbf{v})$  in  $\mathcal{V}'$ , where  $q' \stackrel{\text{def}}{=} (q, \mathbf{I})$  and  $p' \stackrel{\text{def}}{=} (p, M(w))$ .
- (b) If  $q'(\mathbf{0}) \xrightarrow{*} p'(\mathbf{v})$  in  $\mathcal{V}'$ , where  $q' \stackrel{\text{def}}{=} (q, \mathbf{I})$  and  $p' \stackrel{\text{def}}{=} (p, \mathbf{A})$ , then there exists  $w \in T^*$  such that  $M(w) = \mathbf{A}$  and  $p(\mathbf{0}) \xrightarrow{w} q(\mathbf{v})$  in  $\mathcal{V}$ .

*Proof.* (a) By Lemma 3.3,  $\mathcal{V}$  has a path  $w \in T^*$  such that  $w(\mathbf{0}) = \mathbf{v}$ . Let  $k \stackrel{\text{def}}{=} |w|$ . Let  $\mathbf{A}_0 \stackrel{\text{def}}{=} \mathbf{I}$ , and for every  $i \in [k]$  let

$$\mathbf{A}_i \stackrel{\text{def}}{=} M(w_{k-i+1} \cdots w_{k-1} w_k),$$

$$\mathbf{b}_i \stackrel{\text{def}}{=} \mathbf{A}_{i-1} \cdot \Delta(w_{k-i+1}),$$

$$w'_i \stackrel{\text{def}}{=} ((\text{tgt}(w_{k-i+1}), \mathbf{A}_{i-1}), \mathbf{I}, \mathbf{b}_i, (\text{src}(w_{k-i+1}), \mathbf{A}_i)).$$

We claim that  $w' \stackrel{\text{def}}{=} w'_1 w'_2 \cdots w'_k$  is such that  $(q, \mathbf{A}_0) \xrightarrow{w'} (p, \mathbf{A}_k)$  in  $\mathcal{V}'$ . Note that the validity of the claim completes the proof since  $\mathbf{A}_0 = \mathbf{I}$  and  $\mathbf{A}_k = M(w)$ .

It follows immediately from the definition of  $T'$  that  $w'_i \in T'$  for every  $i \in [k]$  and hence that  $w'$  is a path from  $(q, \mathbf{A}_0)$  to  $(p, \mathbf{A}_k)$ . By Lemma 3.3, it remains to show that  $w'(\mathbf{0}) = \mathbf{v}$ :

$$\begin{aligned} w'(\mathbf{0}) &= \sum_{i=1}^k M(w'_{i+1} w'_{i+2} \cdots w'_k) \cdot \Delta(w'_i) && \text{(by Lemma 3.4 applied to } w'(\mathbf{0})\text{)} \\ &= \sum_{i=1}^k \Delta(w'_i) && \text{(by } M(w'_i) = \mathbf{I} \text{ for every } i \in [k]\text{)} \\ &= \sum_{i=1}^k \mathbf{A}_{i-1} \cdot \Delta(w_{k-i+1}) && \text{(by definition of } \Delta(w'_i)\text{)} \\ &= \sum_{i=1}^k M(w_{k-i+2} w_{k-i+1} \cdots w_k) \cdot \Delta(w_{k-i+1}) && \text{(by definition of } \mathbf{A}_{i-1}\text{)} \\ &= \sum_{i=1}^k M(w_{i+1} w_{i+2} \cdots w_k) \cdot \Delta(w_i) && \text{(by inspection of the sum)} \\ &= w(\mathbf{0}) && \text{(by Lemma 3.4 applied to } w(\mathbf{0})\text{)}. \end{aligned}$$

(b) Similarly, by Lemma 3.3, there exists a path  $w'$  of  $\mathcal{V}'$  such that  $w'(\mathbf{0}) = \mathbf{v}$ , and it suffices to exhibit a path  $w \in T^*$  from  $p$  to  $q$  in  $\mathcal{V}$  such that  $w(\mathbf{0}) = \mathbf{v}$  and  $M(w) = \mathbf{A}$ . Let  $k \stackrel{\text{def}}{=} |w'|$ . For every  $i \in [k]$ , let  $w'_i = ((p_i, \mathbf{A}_i), \mathbf{I}, \mathbf{b}_i, (q_i, \mathbf{B}_i))$ . By definition of  $T'$ , for every  $i \in [k]$ , there exists a (possibly non unique) transition  $t_i \in T$  such that  $\text{tgt}(t) = p_i$ ,  $\text{src}(t) = q_i$ ,  $\mathbf{b}_i = \mathbf{A}_i \cdot \Delta(t)$  and  $\mathbf{B}_i = \mathbf{A}_i \cdot M(t)$ . We set  $w \stackrel{\text{def}}{=} t_1 t_2 \cdots t_k$ . It is readily seen that  $w$  is a path from  $p$  to  $q$ . To prove  $w(\mathbf{0}) = \mathbf{v}$  and  $M(w) = \mathbf{A}$ , Lemma 3.4 can be applied as in the previous implication.  $\square$

**3.3. Reachability from an arbitrary configuration.** We now construct the  $\mathbb{Z}$ -VASS  $\mathcal{V}'' = (2d, Q'', T'')$  of Theorem 3.1 which is obtained mostly from  $\mathcal{V}'$ . The states of  $\mathcal{V}''$  are defined as:

$$Q'' \stackrel{\text{def}}{=} Q \cup Q' \cup \overline{Q'} \quad \text{where} \quad \overline{Q'} \stackrel{\text{def}}{=} \{(\overline{q}, \mathbf{A}) : (q, \mathbf{A}) \in Q'\}.$$

To simplify notation, given two vectors  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^d$  we write  $(\mathbf{u}, \mathbf{v})$  for the vector of  $\mathbb{Z}^{2d}$  equal to  $\mathbf{u}$  on the first  $d$  components and equal to  $\mathbf{v}$  on the last  $d$  components. The set  $T''$  consists of four disjoint subsets of transitions  $T_{\text{simul}} \cup T_{\text{end}} \cup T_{\text{mult}} \cup T_{\text{final}}$  working in four sequential stages. Intuitively, these transitions allow (1)  $\mathcal{V}''$  to simulate a path  $w$  of  $\mathcal{V}$  backwards in order to compute  $w(\mathbf{0})$ ; (2) guess the end of this path; (3) compute  $M(w) \cdot \mathbf{u}$  by using the fact that  $M(w)$  is stored in its control-state; and (4) guess the end of this matrix multiplication.

The first set of transitions is defined as:

$$T_{\text{simul}} \stackrel{\text{def}}{=} \{(\text{src}(t), \mathbf{I}, (\mathbf{0}, \Delta(t)), \text{tgt}(t)) : t \in T'\}.$$

Its purpose is to simulate  $T'$  on the last  $d$  counters. The second set is defined as:

$$T_{\text{end}} \stackrel{\text{def}}{=} \{((q, \mathbf{A}), \mathbf{I}, (\mathbf{0}, \mathbf{0}), (\overline{q}, \mathbf{A})) : (q, \mathbf{A}) \in Q'\},$$

and its purpose is to nondeterministically guess the end of a run in  $\mathcal{V}'$  by simply marking  $q$ . The third set is defined as:

$$T_{\text{mult}} \stackrel{\text{def}}{=} \{((\overline{q}, \mathbf{A}), \mathbf{I}, (-\mathbf{e}_i, \mathbf{A} \cdot \mathbf{e}_i), (\overline{q}, \mathbf{A})) : (\overline{q}, \mathbf{A}) \in \overline{Q'}, i \in [d]\} \cup \\ \{((\overline{q}, \mathbf{A}), \mathbf{I}, (\mathbf{e}_i, -\mathbf{A} \cdot \mathbf{e}_i), (\overline{q}, \mathbf{A})) : (\overline{q}, \mathbf{A}) \in \overline{Q'}, i \in [d]\},$$

where  $\mathbf{e}_i$  is the  $i$ -th unit vector such that  $\mathbf{e}_i(i) = 1$  and  $\mathbf{e}_i(j) = 0$  for all  $i \neq j$ . The purpose of  $T_{\text{mult}}$  is to compute  $\mathbf{A} \cdot \mathbf{u}$  from the  $d$  first counters onto the  $d$  last counters. Finally,  $T_{\text{final}}$  is defined as:

$$T_{\text{final}} \stackrel{\text{def}}{=} \{((\overline{q}, \mathbf{A}), \mathbf{I}, (\mathbf{0}, \mathbf{0}), q) : (\overline{q}, \mathbf{A}) \in \overline{Q'}\},$$

and its purpose is to guess the end of the matrix multiplication performed with  $T_{\text{mult}}$ .

We may now prove Theorem 3.1:

*Proof of Theorem 3.1.* First, note that we obtain

$$\begin{aligned} |Q''| &= 2 \cdot |Q'| + |Q| \\ &\leq 3 \cdot |Q| \cdot |\mathcal{M}|, \\ |T''| &= |T'| + |Q'| + 2d \cdot |Q'| + |Q'| \\ &= |T'| + 2(d+1) \cdot |Q'| \\ &= |T'| \cdot |\mathcal{M}| + 2(d+1) \cdot |Q| \cdot |\mathcal{M}| \\ &\leq 4d \cdot |\mathcal{M}| \cdot (|T'| + |Q|). \end{aligned}$$

Moreover, we have:

$$\begin{aligned} \|T''\| &= \max(\|T'\|, \|\mathcal{M}\|) \\ &\leq \max(\|\mathcal{M}\| \cdot \|T\|, \|\mathcal{M}\|) \\ &= \|\mathcal{M}\| \cdot \|T\|. \end{aligned}$$

We conclude by proving that  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$  in  $\mathcal{V}$  if and only if  $q'(\mathbf{u}, \mathbf{0}) \xrightarrow{*} p(\mathbf{0}, \mathbf{v})$  in  $\mathcal{V}''$ , where  $q' \stackrel{\text{def}}{=} (q, \mathbf{I})$ .

$\Rightarrow$ ) By Lemma 3.3, there exists a path  $w$  of  $\mathcal{V}$  such that  $w(\mathbf{u}) = \mathbf{v}$ . By definition of  $T_{\text{simul}}$  and  $T_{\text{end}}$ , and by Proposition 3.5, it is the case that  $q'(\mathbf{u}, \mathbf{0}) \xrightarrow{*} p'(\mathbf{u}, w(\mathbf{0}))$  where  $p' \stackrel{\text{def}}{=} (p, M(w))$ . The transitions of  $T_{\text{mult}}$  allow to transform  $(\mathbf{u}, w(\mathbf{0}))$  into  $(\mathbf{0}, w(\mathbf{0}) + M(w) \cdot \mathbf{u})$ . Thus, using  $T_{\text{final}}$ , we can reach the configuration  $p(w(\mathbf{0}) + M(w) \cdot \mathbf{u})$ . This concludes the proof since  $w(\mathbf{u}) = w(\mathbf{0}) + M(w) \cdot \mathbf{u}$  by Lemma 3.4.

$\Leftarrow$ ) The converse implication follows the same steps as the previous one. It suffices to observe that the first part of a run of  $\mathcal{V}''$  defines the value  $w(\mathbf{0})$ , while the second part of the run defines  $M(w) \cdot \mathbf{u}$ .  $\square$

#### 4. SEMILINEARITY OF AFFINE $\mathbb{Z}$ -VASS

A subset of  $\mathbb{Z}^d$  is called *semilinear* if it is definable by a formula of Presburger arithmetic [Pre29], *i.e.* by a formula of  $\text{FO}(\mathbb{Z}, +, <)$ , the decidable first-order logic over  $\mathbb{Z}$  with addition and order. Semilinear sets capture precisely finite unions of sets of the form  $\mathbf{b} + \mathbb{N} \cdot \mathbf{p}_1 + \mathbb{N} \cdot \mathbf{p}_2 + \dots + \mathbb{N} \cdot \mathbf{p}_k$  with each  $\mathbf{p}_i \in \mathbb{Z}^d$ , and are effectively closed under basic operations such as finite sums, intersection and complement. Those properties make semilinear sets an important tool in many areas of computer science and find use whenever infinite subsets of  $\mathbb{Z}^d$  need to be manipulated.

The results of Section 3 enable us to show that any affine  $\mathbb{Z}$ -VASS with the finite-monoid property has a semilinear reachability relation:

**Theorem 4.1.** *Given an afmp- $\mathbb{Z}$ -VASS  $\mathcal{V} = (d, Q, T)$  and  $p, q \in Q$ , it is possible to compute an existential Presburger formula  $\varphi_{\mathcal{V}, p, q}$  of size at most  $\mathcal{O}(\text{poly}(|\mathcal{V}|, |\mathcal{M}_{\mathcal{V}}|, \log\|\mathcal{M}_{\mathcal{V}}\|))$  such that  $\varphi_{\mathcal{V}, p, q}(\mathbf{u}, \mathbf{v})$  holds if and only if  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$  in  $\mathcal{V}$ .*

*Proof.* By Theorem 3.1, there exist an effectively computable  $\mathbb{Z}$ -VASS  $\mathcal{V}' = (d', Q', T')$  and  $p', q' \in Q'$  such that  $d' = 2 \cdot d$ ,  $|Q'| \leq 3 \cdot |\mathcal{M}| \cdot |Q|$ ,  $|T'| \leq 4d \cdot |\mathcal{M}| \cdot (|Q| + |T|)$ ,  $\|T'\| \leq \|\mathcal{M}\| \cdot \|T\|$  and

$$p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v}) \text{ in } \mathcal{V} \text{ if and only if } p'(\mathbf{u}, \mathbf{0}) \xrightarrow{*} q'(\mathbf{0}, \mathbf{v}) \text{ in } \mathcal{V}'. \quad (4.1)$$

By [HH14, Sect. 3], we can compute an existential Presburger formula  $\psi$  of linear size in  $|\mathcal{V}'|$  such that  $\psi(\mathbf{x}, \mathbf{x}', \mathbf{y}, \mathbf{y}')$  holds if and only if  $p'(\mathbf{x}, \mathbf{x}') \xrightarrow{*} q'(\mathbf{y}, \mathbf{y}')$  in  $\mathcal{V}'$ . By Equation (4.1), the formula  $\varphi_{\mathcal{V}, p, q}(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \psi(\mathbf{x}, \mathbf{0}, \mathbf{0}, \mathbf{y})$  satisfies the theorem.  $\square$

It was observed in [FL02, Boi98] that the reachability relation of a  $\mathbb{Z}$ -VASS  $\mathcal{V} = (d, Q, T)$ , such that  $|Q| = |M(\mathcal{V})| = 1$ , is semilinear if and only if  $\mathcal{M}_{\mathcal{V}}$  is finite. Theorem 4.1 shows that if we do not bound the number of states and matrices, *i.e.* drop the assumption  $|Q| = |M(\mathcal{V})| = 1$ , then  $(\Leftarrow)$  remains true. It is natural to ask whether  $(\Rightarrow)$  also remains true.

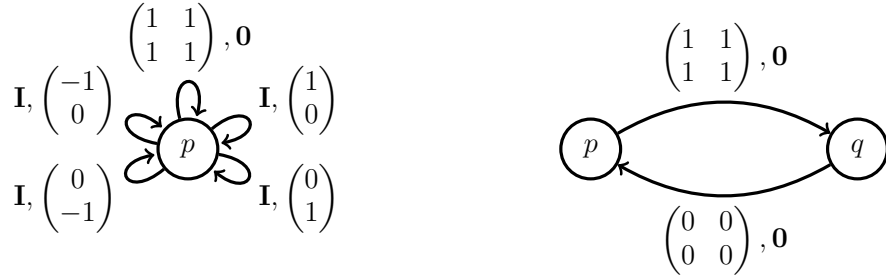


FIGURE 3. Examples of affine  $\mathbb{Z}$ -VASS with infinite monoids and semilinear reachability relations.

Let  $\mathcal{V}_1$  and  $\mathcal{V}_2$  be the affine  $\mathbb{Z}$ -VASS illustrated in Figure 3 from left to right respectively. Note that  $\mathcal{M}_{\mathcal{V}_1}$  and  $\mathcal{M}_{\mathcal{V}_2}$  are both infinite due to the matrix made only of 1s. Moreover, the reachability relations of  $\mathcal{V}_1$  and  $\mathcal{V}_2$  are semilinear since the former can reach any target configuration from any initial configuration, and since the latter can only generate finitely many vectors due to the zero matrix. Since  $\mathcal{V}_1$  has a single control-state,  $|M(\mathcal{V}_1)| = |M(\mathcal{V}_2)| = 2$  and  $\Delta(\mathcal{V}_2) = \{\mathbf{0}\}$ , any simple natural extension of the characterization of semilinearity in terms of the number of control-states, matrices and vectors fails.

It is worth noting that an affine  $\mathbb{Z}$ -VASS with an infinite monoid may have a non semilinear reachability relation. Indeed, Figure 2 depicts a transfer + copy  $\mathbb{Z}$ -VASS with an infinite monoid and such that  $\{\mathbf{v} : p(1, 1) \xrightarrow{*} q(\mathbf{v})\} = \{(2^n, 2^n) : n \in \mathbb{N}\}$ , which is known to be non semilinear. Moreover, this proves that even the reachability set from  $p(1, 1)$  is not semilinear.

## 5. COMPLEXITY OF REACHABILITY FOR AFMP- $\mathbb{Z}$ -VASS

In this section, we use the results of Section 3 to show that reachability belongs to PSPACE for a large class of afmp- $\mathbb{Z}$ -VASS encompassing all variants discussed in Section 2. Moreover, we give a novel proof to the known NP membership of reachability for reset  $\mathbb{Z}$ -VASS.

For every finite set  $G_d \subseteq \mathbb{Z}^{d \times d}$ , let  $\langle G_d \rangle$  be the monoid generated by  $G_d$ . We have:

**Theorem 5.1.** *Let  $\mathcal{C} = \bigcup_{d \geq 1} \mathcal{C}_d$  be a class of matrices such that  $\mathcal{C}_d$  is finite for every  $d \geq 1$ . It is the case that  $\text{Reach}_{\mathcal{C}} \in \text{PSPACE}$  if there exists a polynomial poly such that  $|\langle G_d \rangle| + \|\langle G_d \rangle\| \leq 2^{\text{poly}(d + \log \|G_d\|)}$  for every  $d \geq 1$  and every finite set  $G_d$  such that  $\langle G_d \rangle \subseteq \mathcal{C}_d$ .*

*Proof.* Let  $\mathcal{V} = (d, Q, T)$  be an affine  $\mathbb{Z}$ -VASS from class  $\mathcal{C}$ . Let  $\mathcal{V}' = (d, Q', T')$  be the  $\mathbb{Z}$ -VASS obtained from  $\mathcal{V}$  in Theorem 3.1. Recall that, by Theorem 3.1,  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$  in  $\mathcal{V}$  if and only if  $p'(\mathbf{u}, \mathbf{0}) \xrightarrow{*} q'(\mathbf{0}, \mathbf{v})$  in  $\mathcal{V}'$ . Therefore, it suffices to check the latter for determining reachability in  $\mathcal{V}$ .

We invoke a result of [BFG<sup>+</sup>15] on the flattability of  $\mathbb{Z}$ -VASS. By [BFG<sup>+</sup>15, Prop. 3],  $p'(\mathbf{x}) \xrightarrow{*} q'(\mathbf{y})$  in  $\mathcal{V}'$  if and only if there exist  $k \leq |T'|$ ,  $\alpha_0, \beta_1, \alpha_1, \dots, \beta_k, \alpha_k \in (T')^*$  and  $\mathbf{e} \in \mathbb{N}^k$  such that

- (i)  $p'(\mathbf{x}) \xrightarrow{\alpha_0 \beta_1^{\mathbf{e}(1)} \alpha_1 \dots \beta_k^{\mathbf{e}(k)}} q'(\mathbf{y})$  in  $\mathcal{V}'$ ,
- (ii)  $\beta_i$  is a cycle for every  $i \in [k]$ , and
- (iii)  $\alpha_0 \beta_1 \alpha_1 \dots \beta_k \alpha_k$  is a path from  $p'$  to  $q'$  of length at most  $2 \cdot |Q'| \cdot |T'|$ .

For every  $w \in (T')^*$ , let  $\Delta(w) \stackrel{\text{def}}{=} \sum_{i=1}^{|w|} \Delta(w_i)$ . By Lemma 3.4 (see the remark below the proof of Lemma 3.4), we have  $w(\mathbf{u}) = \mathbf{u} + \Delta(w)$  for every  $\mathbf{u} \in \mathbb{Z}^d$ . Thus, by Lemma 3.3, checking (i), assuming (iii), amounts to testing whether  $\mathbf{e}$  is a solution of the following system of linear Diophantine equations:

$$\mathbf{x} + \sum_{i=0}^k \Delta(\alpha_i) + (\Delta(\beta_1) \quad \Delta(\beta_2) \quad \cdots \quad \Delta(\beta_k)) \cdot \mathbf{e} = \mathbf{y}. \quad (5.1)$$

Let  $G_d \stackrel{\text{def}}{=} M(\mathcal{V})$ . Note that  $\|G_d\| \leq \|T\|$  and that  $\langle G_d \rangle = \mathcal{M}_{\mathcal{V}}$ . Let  $m \stackrel{\text{def}}{=} 2 \cdot |Q'| \cdot |T'|$ . By Theorem 3.1, we have  $m \leq 48d \cdot |\mathcal{M}|^2 \cdot |Q|^2 \cdot |T|$ . Thus, since  $\langle G_d \rangle$  is a submonoid of  $\mathcal{C}_d$ , and by assumption on  $\mathcal{C}_d$ , we have

$$m \leq 48d \cdot \left(2^{\text{poly}(d+\log\|T\|)}\right)^2 \cdot |Q|^2 \cdot |T|.$$

Thus,  $m$  is exponential in  $|\mathcal{V}|$ .

We describe a polynomial-space non deterministic Turing machine  $\mathcal{A}$  for testing whether  $p'(\mathbf{x}) \xrightarrow{*} q'(\mathbf{y})$  in  $\mathcal{V}'$ . The proof follows from  $\text{NPSpace} = \text{PSPACE}$ . Machine  $\mathcal{A}$  guesses  $k \leq |T'|$ , a path  $\pi = \alpha_0\beta_1\alpha_1 \cdots \beta_k\alpha_k$  of length at most  $m$  from  $p'$  to  $q'$ , and  $\mathbf{e} \in \mathbb{N}^k$ , and tests whether (5.1) holds for  $\pi$ . Note that we are not given  $\mathcal{V}'$ , but  $\mathcal{V}$ , so we must be careful for the machine to work in polynomial space.

Instead of fully constructing  $\mathcal{V}'$  and fully guessing  $\pi$ , we do both on the fly, and also construct  $\Delta(\alpha_0), \Delta(\beta_1), \dots, \Delta(\beta_k), \Delta(\alpha_k)$  on the fly as partial sums as we guess  $\pi$ . Note that to ensure that each  $\beta_i$  is a cycle, we do not need to fully store  $\beta_i$  but only its starting control-state. Moreover, note that  $\|\Delta(\alpha_i)\|, \|\Delta(\beta_i)\| \leq m \cdot \|T'\|$  for every  $i$ . By Theorem 3.1 and by assumption on  $\mathcal{C}_d$ , we have

$$\begin{aligned} \|T'\| &\leq \|\langle G_d \rangle\| \cdot \|T\| \\ &\leq 2^{\text{poly}(d+\log\|T\|)} \cdot \|T\|. \end{aligned}$$

Hence, each  $\alpha_i$  and  $\beta_i$  has a binary representation of polynomial size in  $|\mathcal{V}|$ .

By [CH16, Prop. 4], (5.1) has a solution if and only if it has a solution  $\mathbf{e} \in \mathbb{N}^k$  such that

$$\|\mathbf{e}\| \leq \left( (k+1) \cdot \max\{\|\Delta(\beta_i)\| : i \in [k]\} + \|\mathbf{x}\| + \|\mathbf{y}\| + \sum_{i=0}^k \|\Delta(\alpha_i)\| + 1 \right)^{d'}.$$

Since  $d' = 2 \cdot d$ , this means that we can guess a vector  $\mathbf{e} \in \mathbb{N}^k$  whose binary representation is of polynomial size, and that we can thus evaluate (5.1) in polynomial time.  $\square$

**Corollary 5.2.** *The reachability problem for nonnegative afmp- $\mathbb{Z}$ -VASS is in PSPACE, and hence in particular for reset, permutation, transfer, copy and copyless  $\mathbb{Z}$ -VASS.*

*Proof.* Let  $\mathcal{C} = \bigcup_{d \geq 1} \mathcal{C}_d$  be a class of nonnegative matrices. Let  $d \geq 1$  and let  $G_d$  be a finite set of matrices such that  $\langle G_d \rangle \subseteq \mathcal{C}_d$ . By [WS91, Theorem A.2], whose proof appears in [Web87] written by one of the same authors, we have:

$$\begin{aligned} |\langle G_d \rangle| &\leq \|G_d\|^{d^2 \cdot (d-1)} \cdot 5^{d^3/2} \cdot d^{d^3} \cdot d^2 = 2^{d^2 \cdot (d-1) \cdot \log\|G_d\| + (d^3/2) \cdot \log 5 + d^3 \cdot \log d + 2 \cdot \log d}, \\ \|\langle G_d \rangle\| &\leq \|G_d\|^{d-1} \cdot 5^{d/2} \cdot d^d = 2^{(d-1) \cdot \log\|G_d\| + (d/2) \cdot \log 5 + d \cdot \log d}. \end{aligned}$$

Thus,  $\mathcal{C}$  satisfies the requirements of Theorem 5.1. To complete the proof, observe that determining whether  $\mathcal{M}_{\mathcal{V}}$  is finite can be done in time  $\mathcal{O}(d^6 \cdot |T|)$ , again by [WS91, Theorem A.2] and [Web87].

Note that this proof applies to reset, permutation, transfer, copy and copyless classes, respectively, as they are all nonnegative. However, there is a much simpler argument for these specific classes. Indeed, their matrices all have a max-norm of at most 1 and thus their monoids contain at most  $2^{d^2}$  matrices.  $\square$

**Theorem 5.3** [HH14]. *The reachability problem for reset  $\mathbb{Z}$ -VASS belongs to NP.*

*Proof.* Let  $\mathcal{V} = (d, Q, T)$  be a reset  $\mathbb{Z}$ -VASS. The proof does not follow immediately from Theorem 3.1 because  $\mathcal{M}_{\mathcal{V}}$  can be of size up to  $2^d$ . We will analyze the construction used in the proof of Theorem 3.1, where reachability in  $\mathcal{V}$  is effectively reduced to reachability in a  $\mathbb{Z}$ -VASS  $\mathcal{V}' = (d', Q', T')$ . Recall that  $Q' = (Q \times \mathcal{M}_{\mathcal{V}}) \cup (\bar{Q} \times \mathcal{M}_{\mathcal{V}}) \cup Q$ , and thus that the size of  $\mathcal{V}'$  depends only on the sizes of  $Q$  and  $\mathcal{M}_{\mathcal{V}}$ .

It follows from the proof of Theorem 3.1 and Proposition 3.5 that for every run  $q'(\mathbf{u}, \mathbf{0}) \xrightarrow{*} p(\mathbf{0}, \mathbf{v})$  in  $\mathcal{V}'$  where  $q' \stackrel{\text{def}}{=} (q, \mathbf{I})$ , there is a corresponding run  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$  in  $\mathcal{V}$  for some  $w \in T^*$  of length  $k \geq 0$ . Moreover, the  $i^{\text{th}}$  matrix occurring within the control-states of this run are of the form  $\mathbf{A}_i$  where  $\mathbf{A}_i = \mathbf{A}_{i-1} \cdot \mathbf{B}$  for some  $\mathbf{B} \in \mathcal{M}_{\mathcal{V}}$ . Since  $\mathcal{M}_{\mathcal{V}}$  consists of reset matrices, it holds that  $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_k$  is monotonic, *i.e.* if  $\mathbf{A}_{i-1}$  has a 0 somewhere on its diagonal, then  $\mathbf{A}_i$  also contains 0 in that position. It follows that  $\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_k$  is made of at most  $d + 1$  distinct matrices.

To prove the NP upper bound we proceed as follows. We guess at most  $d + 1$  matrices of  $\mathcal{M}_{\mathcal{V}}$  that could appear in sequence  $\mathbf{A}_0, \mathbf{A}_1, \dots, \mathbf{A}_k$ . We construct the  $\mathbb{Z}$ -VASS  $\mathcal{V}'$  as in Theorem 3.1, but we discard each control-state of  $Q'$  containing a matrix not drawn from the guessed matrices. Since the constructed  $\mathbb{Z}$ -VASS is of polynomial size, reachability can be verified in NP [HH14].  $\square$

**Remark 5.4.** Observe that the proof of Theorem 5.3 holds for any class of affine  $\mathbb{Z}$ -VASS with a finite monoid such that every path of its Cayley graph contains at most polynomially many different vertices. For a reset  $\mathbb{Z}$ -VASS of dimension  $d$ , the number of vertices on every path of the Cayley graph is bounded by  $d + 1$ .

## 6. HARDNESS RESULTS FOR REACHABILITY

It is known that the reachability problem for  $\mathbb{Z}$ -VASS is already NP-hard [HH14], which means that reachability is NP-hard for all classes of affine  $\mathbb{Z}$ -VASS. In this section, we show that PSPACE-hardness holds for some classes, matching the PSPACE upper bound derived in Section 5. Moreover, we observe that reachability is undecidable for transfer + copy  $\mathbb{Z}$ -VASS.

**Theorem 6.1.** *The reachability problem for permutation  $\mathbb{Z}$ -VASS is PSPACE-hard.*

*Proof.* We give a reduction from the membership problem of linear bounded automata, which is known to be PSPACE-complete (see, *e.g.*, [HU79, Sect. 9.3 and 13]). Let  $\mathcal{A} = (P, \Sigma, \Gamma, \delta, q^{\text{ini}}, q^{\text{acc}}, q^{\text{rej}})$  be a linear bounded automaton, where:

- $P$  is the set of states,
- $\Sigma \subseteq \Gamma$  is the input alphabet,
- $\Gamma$  is the tape alphabet,
- $\delta$  is the transition function, and
- $q^{\text{ini}}, q^{\text{acc}}, q^{\text{rej}}$  are the initial, accepting and rejecting states respectively.

The transition function is a mapping  $\delta : P \times \Gamma \rightarrow P \times \Gamma \times \{\text{LEFT}, \text{RIGHT}\}$ . The intended meaning of a transition  $\delta(p, a) = (q, b, D)$  is that whenever  $\mathcal{A}$  is in state  $p$  and holds letter  $a$  at the current position of its tape, then  $\mathcal{A}$  overwrites  $a$  with  $b$  and moves to state  $q$  and to the next tape position in direction  $D$ .

Let us fix a word  $w \in \Sigma^*$  of length  $n$  that we will check for membership. We construct a permutation  $\mathbb{Z}$ -VASS  $\mathcal{V} = (d, Q, T)$  and configurations  $r(\mathbf{u})$  and  $r'(\mathbf{0})$  such that  $\mathcal{A}$  accepts  $w$  if and only if  $r(\mathbf{u}) \xrightarrow{*} r'(\mathbf{0})$ .

We set  $d \stackrel{\text{def}}{=} n \cdot |\Gamma| + 1$  and associate a counter to each position of  $w$  and each letter of the tape alphabet  $\Gamma$ , plus one additional counter. For readability, we denote these counters respectively as  $x_{i,a}$  and  $y$ , where  $i \in [n]$  and  $a \in \Gamma$ . The idea is to maintain, for every  $i \in [n]$ , a single non zero counter among  $\{x_{i,a} : a \in \Gamma\}$  in order to represent the current letter in the  $i^{\text{th}}$  tape cell of  $\mathcal{A}$ . The initial vector is  $\mathbf{u} \in \{0, 1\}^d$  such that  $\mathbf{u}(y) = n$  and  $\mathbf{u}(x_{i,a}) = 1$  if and only if  $w_i = a$  for every  $i \in [n]$  and  $a \in \Gamma$ . The invariant that will be maintained during all runs is  $y = \sum_{i,a} x_{i,a}$ .

The control-states of  $\mathcal{V}$  are defined as:

$$Q \stackrel{\text{def}}{=} \{r_{p,i} : p \in P, i \in [n]\} \cup \{r_{a,i} : a \in \Gamma, i \in [n]\} \cup \{r_{\text{acc}}\}.$$

The purpose of each state of the form  $r_{p,i}$  is to store the current state  $p$  and head position  $i$  of  $\mathcal{A}$ . States of the form  $r_{a,i}$  will be part of a gadget testing whether  $\mathcal{A}$  is simulated faithfully.

We associate a transition to every triple  $(p, a, i) \in P \times \Gamma \times [n]$ , which denotes a configuration of  $\mathcal{A}$ : the automaton is in state  $p$  in position  $i$ , where letter  $a$  is stored. Let us fix a transition  $\delta(p, a) = (q, b, D)$ ; and let  $j \stackrel{\text{def}}{=} i + 1$  if  $D = \text{RIGHT}$ , and  $j \stackrel{\text{def}}{=} i - 1$  if  $D = \text{LEFT}$ . For every  $i \in [n]$ , if  $j \in [n]$ , then we add to  $T$  the transition

$$(r_{p,i}, \mathbf{A}, \mathbf{a}, r_{q,j})$$

where  $\mathbf{A}$  is a permutation matrix that swaps the values of  $x_{i,a}$  and  $x_{i,b}$ ; and  $\mathbf{a}$  is the vector whose only nonzero components are  $\mathbf{a}(x_{i,b}) = 1$  and  $\mathbf{a}(y) = 1$ . The transition is depicted on the left of Figure 4 (for  $D = \text{RIGHT}$ ). Notice that all transitions maintain the invariant  $y = \sum_{i,a} x_{i,a}$ .

The purpose of the swap is to simulate the transition of  $\mathcal{A}$ , upon reading  $a$  in tape cell  $i$  and state  $p$ , by moving the contents from  $x_{i,a}$  to  $x_{i,b}$ . Note that this transition may be faulty, *i.e.* it can simulate reading letter  $a$  even though tape cell  $i$  contains another letter. The purpose of the vector  $\mathbf{a}$  is to detect such faulty behaviour: if the cell  $i$  does not contain  $a$ , then more than one counter among  $\{x_{i,a} : a \in \Gamma\}$  will be a nonzero counter.

Recall that  $y = \sum_{i,a} x_{i,a}$ . We conclude that  $\mathcal{A}$  accepts  $w$  if and only if there exist  $j \in [n]$ ,  $\mathbf{u}' \in \mathbb{N}^d$  and  $a_1, a_2, \dots, a_n \in \Gamma$  such that

$$r_{q_{\text{ini}},1}(\mathbf{u}) \xrightarrow{*} r_{q_{\text{acc}},j}(\mathbf{u}') \text{ and } \mathbf{u}'(y) = \sum_{i \in [d]} \mathbf{u}'(x_{i,a_i}).$$

To test whether such index  $j$ , vector  $\mathbf{u}'$  and letters  $a_1, a_2, \dots, a_n$  exist, we add some transitions to  $T$  as illustrated on the right of Figure 4. For every  $i \in [n]$  and every  $a \in \Gamma$ , we add to  $T$  the transitions  $(r_{q_{\text{acc}},i}, \mathbf{I}, \mathbf{0}, r_{a,1})$ . For every  $i \in [n]$  and  $a \in \Gamma$ , we add to  $T$  the transitions  $(r_{a,i}, \mathbf{I}, \mathbf{b}, r_{a,i})$  where  $\mathbf{b}$  is the vector whose only non zero components are  $\mathbf{b}(x_{i,a}) = \mathbf{b}(y) = -1$ . Moreover, if  $i < n$ , then for every  $a, b \in \Gamma$  we also add transitions  $(r_{a,i}, \mathbf{I}, \mathbf{0}, r_{b,i+1})$ . Finally, for all  $a \in \Gamma$ , we also add transitions  $(r_{a,n}, \mathbf{I}, \mathbf{0}, r_{\text{acc}})$ . The purpose of these transitions is to guess for each  $i$  some letter  $a_i$  and simultaneously decrease  $x_{i,a_i}$

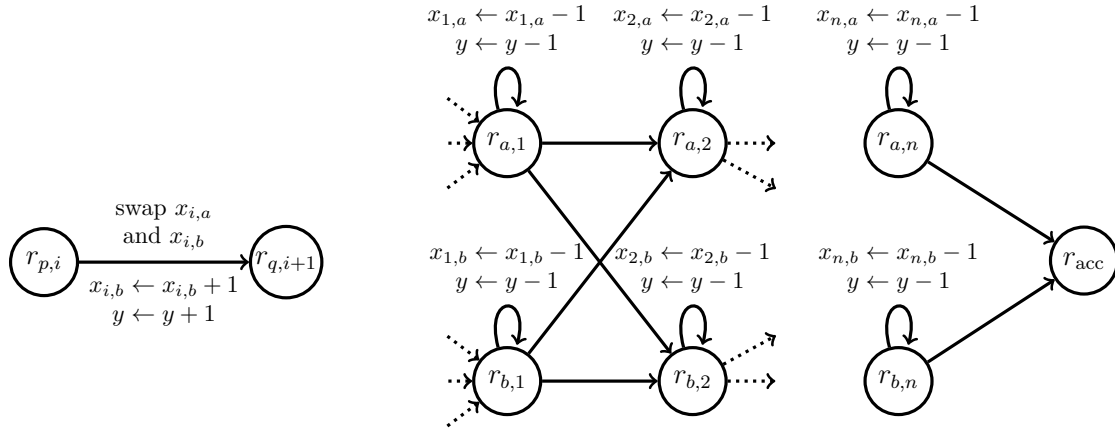


FIGURE 4. *Left*: transitions of  $\mathcal{V}$  simulating transition  $\delta(p, a) = (q, b, \text{RIGHT})$  of  $\mathcal{A}$ . *Right*: gadget verifying whether the accepting state has been reached with no error during the simulation. For readability, we assume  $\Gamma = \{a, b\}$  in the right gadget.

and  $y$ . We do this for each  $i$  starting from 1 to  $n$  and in the end we move to the state  $r_{\text{acc}}$ . We conclude that  $\mathcal{A}$  accepts  $w$  if and only if  $r_{q_{\text{ini}},1}(\mathbf{u}) \xrightarrow{*} r_{\text{acc}}(\mathbf{0})$  in  $\mathcal{V}$ .  $\square$

**Corollary 6.2.** *The reachability problem is PSPACE-complete for permutation  $\mathbb{Z}$ -VASS, transfer  $\mathbb{Z}$ -VASS and copy  $\mathbb{Z}$ -VASS.*

*Proof.* PSPACE-hardness for permutation  $\mathbb{Z}$ -VASS was shown in Theorem 6.1, and the upper bound for transfer  $\mathbb{Z}$ -VASS and copy  $\mathbb{Z}$ -VASS follows from Theorem 5.1. It remains to observe that permutation matrices are also transfer and copy matrices.  $\square$

**Proposition 6.3.** *The reachability problem for transfer + copy  $\mathbb{Z}$ -VASS is undecidable, even when restricted to three counters.*

*Proof.* Reichert [Rei15] gives a reduction from the Post correspondence problem over the alphabet  $\{0, 1\}$  to reachability in affine  $\mathbb{Z}$ -VASS with two counters. The trick of the reduction

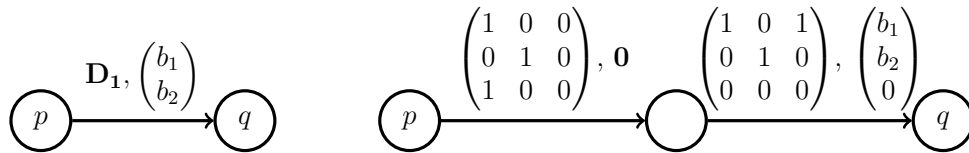


FIGURE 5. Gadget (on the right) made of copy and transfer transitions simulating the doubling transition on the left.

is to represent two binary sequences as the natural numbers the sequences encode, one in each counter. If we add an artificial 1 at the beginning of the two binary sequences, then these sequences are uniquely determined by their numerical values. We only need to be able to double the counter values, which corresponds to shifting the sequences. This can be achieved using the following matrices:

$$\mathbf{D}_1 \stackrel{\text{def}}{=} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \mathbf{D}_2 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$



The only matrices used in the construction of Reichert are  $\mathbf{I}$ ,  $\mathbf{D}_1$  and  $\mathbf{D}_2$ . The last two matrices can be simulated by a gadget made of copy and transfer matrices and by introducing a third counter. This gadget is depicted in Figure 5 for the case of matrix  $\mathbf{D}_1$ . The other gadget is symmetric. Note that if a run enters control-state  $p$  of the gadget with vector  $(x, y, 0)$ , then it leaves control-state  $q$  in vector  $(2x + b_1, y + b_2, 0)$  as required.  $\square$

**Remark 6.4.** The coverability problem for nonnegative affine VASS is known to be decidable in Ackermann time [FFSPS11]. Recall that coverability and reachability are inter-reducible for affine  $\mathbb{Z}$ -VASS. Thus, Proposition 6.3 gives an example of a decision problem, namely coverability, which is more difficult for affine  $\mathbb{Z}$ -VASS than for affine VASS.

## 7. REACHABILITY BEYOND FINITE MONOIDS

Thus far, we have shown, on the one hand, that reachability is decidable for affine  $\mathbb{Z}$ -VASS with the finite-monoid property, and, on the other hand, that reachability is undecidable for arbitrary affine  $\mathbb{Z}$ -VASS. This raises the question of whether there is a decidability dichotomy between classes of finite and infinite monoids, *i.e.* whether reachability is undecidable for *every* class of infinite monoids. In this section, we show that this is not the case: we exhibit a non-trivial class of infinite monoids for which affine  $\mathbb{Z}$ -VASS reachability is *decidable*. In other words, the top rectangular region of Figure 1 is *not* equal to the red ellipse, which answers a question we left open in [BHM18]. The class of affine  $\mathbb{Z}$ -VASS will have a particular shape, namely, the matrix monoids have a single generator. More formally, we say that a class of matrices  $C = \bigcup_{d \geq 1} C_d$  is *monogenic* if each monoid  $C_d$  is generated by a single matrix. In the second part of this section we prove that reachability is in general undecidable for monogenic classes.

**7.1. Decidability for a class of affine  $\mathbb{Z}$ -VASS with infinite monoids.** Let  $C_d$  be the monoid generated by the (nonnegative) matrix  $\mathbf{J}_d \in \mathbb{N}^{d \times d}$  whose entries are all equal to 1. Clearly,  $C_d$  is infinite for every  $d \geq 2$  since  $(\mathbf{J}_d)^n$  is the matrix whose entries are all equal to  $d^n$ . Let  $C_{\mathbf{J}} = \bigcup_{d \geq 1} C_d$ . The rest of this section is devoted to proving the following theorem:

**Theorem 7.1.** *The reachability problem  $Reach_{C_{\mathbf{J}}}$  is decidable.*

Let  $\mathcal{V} = (d, Q, T)$  be an affine  $\mathbb{Z}$ -VASS belonging to  $C_{\mathbf{J}}$ . We will simply write  $\mathbf{J}$  instead of  $\mathbf{J}_d$  as  $d$  is implicit from the dimension of  $\mathcal{V}$ . Observe that we can assume w.l.o.g. that for every transition  $(p, \mathbf{A}, \mathbf{b}, q) \in T$  either  $\mathbf{A} = \mathbf{I}$  or  $\mathbf{b} = \mathbf{0}$ , *i.e.* each transition either performs a transformation of the form  $\mathbf{x} \leftarrow \mathbf{x} + \mathbf{b}$  or  $\mathbf{x} \leftarrow \mathbf{A} \cdot \mathbf{x}$ . Indeed, by adding an extra state  $r$ , we can always split such a transition into two transitions  $(p, \mathbf{A}, \mathbf{0}, r)$  and  $(r, \mathbf{I}, \mathbf{b}, q)$ . We can further assume w.l.o.g. that  $\mathbf{I}$  and  $\mathbf{J}$  are the only matrices occurring in  $\mathcal{V}$ . Indeed, if  $T$  contains a transition  $t = (p, \mathbf{A}, \mathbf{b}, q)$  where  $\mathbf{A} \notin \{\mathbf{I}, \mathbf{J}\}$ , then  $\mathbf{A} = \mathbf{J}^n$  for some  $n \geq 2$  and  $\mathbf{b} = \mathbf{0}$ . Thus, we can simply replace  $t$  by a sequence of transitions  $t_1, t_2, \dots, t_n$  leading from  $p$  to  $q$  and such that  $M(t_i) = \mathbf{J}$  and  $\Delta(t_i) = \mathbf{0}$  for every  $i \in [n]$ .

Let  $T_{\mathbf{I}}$  and  $T_{\mathbf{J}}$  denote the (maximal) subsets of  $T$  of transitions with matrix  $\mathbf{I}$  and  $\mathbf{J}$  respectively. Note that  $T_{\mathbf{I}}$  and  $T_{\mathbf{J}}$  form a partition of  $T$ . We will write  $\xrightarrow{S}$  and  $\xrightarrow{S^*}$  to denote respectively the restriction of  $\rightarrow$  and  $\xrightarrow{*}$  to transitions of a set  $S$ . We give a simple characterization of reachability in  $\mathcal{V}$ :

**Proposition 7.2.** *For all configurations  $p(\mathbf{u})$  and  $q(\mathbf{v})$  of  $\mathcal{V}$ ,  $p(\mathbf{u}) \xrightarrow{*} q(\mathbf{v})$  if and only if:*

- (1)  $p(\mathbf{u}) \xrightarrow{T_{\mathbf{I}}^*} q(\mathbf{v})$ ; or  
(2)  $p(\mathbf{u}) \xrightarrow{*} r'(\mathbf{w}) \xrightarrow{T_{\mathbf{J}}} r(\mathbf{J} \cdot \mathbf{w}) \xrightarrow{T_{\mathbf{I}}^*} q(\mathbf{v})$  for some  $r, r' \in Q$  and  $\mathbf{w} \in \mathbb{Z}^d$ .

*Proof.*  $\Leftarrow$ ) Immediate.

$\Rightarrow$ ) Assume that  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$  for some  $w \in T^*$ . If  $w$  does not contain any transition from  $T_{\mathbf{J}}$ , then (1) holds and we are done. Thus, suppose that  $w$  contains at least one transition from  $T_{\mathbf{J}}$ . Let  $t \in T_{\mathbf{J}}$  be the last such transition occurring in  $w$ . Recall that, by assumption,  $M(t) = \mathbf{J}$  and  $\Delta(t) = \mathbf{0}$ . Therefore, we are done since there exist  $r, r' \in Q$  and  $\mathbf{w} \in \mathbb{Z}^d$  such that

$$p(\mathbf{u}) \xrightarrow{*} r'(\mathbf{w}) \xrightarrow{t} r(\mathbf{J} \cdot \mathbf{w}) \xrightarrow{T_{\mathbf{I}}^*} q(\mathbf{v}). \quad \square$$

In order to prove that  $\text{Reach}_{\mathcal{C}_{\mathbf{J}}}$  is decidable, it suffices to show that there exist procedures to decide the two conditions of Proposition 7.2. Testing condition (1) amounts to  $\mathbb{Z}$ -VASS reachability, which belongs to NP [HH14]. Indeed, any run restricted to  $T_{\mathbf{I}}$  is a run of the  $\mathbb{Z}$ -VASS induced by  $T_{\mathbf{I}}$ . Thus, in the rest of the proof, we focus on showing how to test condition (2).

For this purpose, let us introduce an auxiliary model. An *affine one-counter  $\mathbb{Z}$ -net* is a pair  $(P, U)$  where

- $P$  is a finite set of *states*, and
- $U \subseteq Q \times \{+, \cdot\} \times \mathbb{Z} \times Q$  is a finite set of *transitions*.

Furthermore, for every transition  $t = (p, \otimes, c, q)$ , we write  $p(n) \xrightarrow{t} q(m)$  if  $m = n \otimes c$ . The notions of runs and reachability are defined accordingly as for affine  $\mathbb{Z}$ -VASS. These machines are a special case of one-counter register machines with polynomial updates whose reachability problem belongs to PSPACE [FGH13], *i.e.* we only allow the counter to be multiplied or incremented by constants, whereas the model of [FGH13] allows to update the counter by a polynomial such as  $x^2$  or  $x^3 - x + 1$ .

For every  $\mathbf{v} \in \mathbb{Z}^d$ , let

$$\delta(\mathbf{v}) \stackrel{\text{def}}{=} \sum_{i=1}^d \mathbf{v}(i).$$

Consider the transitions  $T$  in the affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$ . For every transition  $t \in T$ , let  $\bar{t}$  be defined as:

$$\bar{t} \stackrel{\text{def}}{=} \begin{cases} (p, +, \delta(\Delta(t)), q) & \text{if } t \in T_{\mathbf{I}}, \\ (p, \cdot, d, q) & \text{if } t \in T_{\mathbf{J}}, \end{cases}$$

where  $p = \text{src}(t)$  and  $q = \text{tgt}(t)$ .

Let  $\mathcal{W} = (Q, \bar{T})$  be the affine one-counter  $\mathbb{Z}$ -net obtained from  $\mathcal{V} = (d, Q, T)$  by keeping the same states and taking  $\bar{T} \stackrel{\text{def}}{=} \{\bar{t} : t \in T\}$ . We write  $\bar{w} \in \bar{T}^*$  to denote the (unique) sequence of transitions in  $\mathcal{W}$  corresponding to the sequence  $w \in T^*$  of  $\mathcal{V}$ . Let us observe the following correspondence between  $\mathcal{V}$  and  $\mathcal{W}$ :

**Lemma 7.3.** *For every  $p, q \in Q$ ,  $\mathbf{u} \in \mathbb{Z}^d$ ,  $m \in \mathbb{Z}$  and  $w \in T^*$ , we have  $p(\delta(\mathbf{u})) \xrightarrow{\bar{w}} q(m)$  in  $\mathcal{W}$  if and only if  $p(\mathbf{u}) \xrightarrow{w} q(\mathbf{v})$  in  $\mathcal{V}$  for some  $\mathbf{v} \in \mathbb{Z}^d$  such that  $\delta(\mathbf{v}) = m$ .*

*Proof.* The claim follows from a simple induction on  $|w|$ . □

We may now prove Theorem 7.1.

*Proof of Theorem 7.1.* Recall that it suffices to show how to decide condition (2) of Proposition 7.2. By definition of  $\mathbf{J}$ , this condition is equivalent to determining whether there exist  $r \in Q$  and  $n \in \mathbb{Z}$  such that

$$p(\mathbf{u}) \xrightarrow{T^* \cdot T_{\mathbf{J}}} r(n, n, \dots, n) \xrightarrow{T_{\mathbf{I}}^*} q(\mathbf{v}).$$

Let  $S = \{m \in \mathbb{Z} : \exists n \in \mathbb{Z} (m = d \cdot n) \wedge \bigvee_{r \in Q} r(n, n, \dots, n) \xrightarrow{T_{\mathbf{I}}^*} q(\mathbf{v})\}$ . As we mentioned earlier,  $\mathcal{V}$  can be seen as a standard  $\mathbb{Z}$ -VASS when restricted to  $T_{\mathbf{I}}$ . Since the reachability relation of any  $\mathbb{Z}$ -VASS is effectively semilinear [HH14], the set  $S$  is also effectively semilinear.

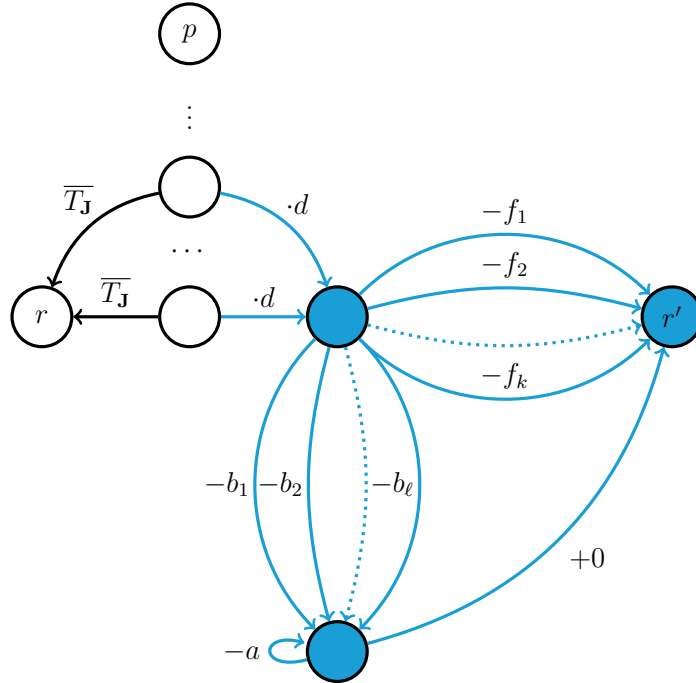


FIGURE 6. Affine one-counter  $\mathbb{Z}$ -net  $\mathcal{W}$  extended with a gadget subtracting a number of  $S$  from some transition of  $\overline{T_{\mathbf{J}}}$  leading to  $r$ . The gadget is depicted in colour. Transitions connecting  $\mathcal{W}$  to the gadget are labeled with “ $\cdot d$ ” as this is the effect of every transition of  $\overline{T_{\mathbf{J}}}$ .

By Lemma 7.3, we have  $p(\mathbf{u}) \xrightarrow{T^* \cdot T_{\mathbf{J}}} r(n, n, \dots, n)$  if and only if  $p(\delta(\mathbf{u})) \xrightarrow{\overline{T^* \cdot \overline{T_{\mathbf{J}}}} r(d \cdot n)$ . Indeed, the direction  $(\Rightarrow)$  is immediate. To prove the implication  $(\Leftarrow)$  suppose  $p(\delta(\mathbf{u})) \xrightarrow{\overline{T^* \cdot \overline{T_{\mathbf{J}}}} r(d \cdot n)$ . By Lemma 7.3 we have  $p(\mathbf{u}) \xrightarrow{T^* \cdot T_{\mathbf{J}}} r(\mathbf{v})$  such that  $\delta(\mathbf{v}) = d \cdot n$ . By definition the last transition is  $r'(\mathbf{w}) \xrightarrow{t} r(\mathbf{J} \cdot \mathbf{w})$ , where  $\mathbf{v} = \mathbf{J} \cdot \mathbf{w}$ . By definition of  $\mathbf{J}$ :  $\mathbf{v} = (\delta(\mathbf{w}), \dots, \delta(\mathbf{w}))$ . Since  $\delta(\mathbf{v}) = d \cdot n$  we get  $\mathbf{v} = (n, n, \dots, n)$ .

Thus, it suffices to test whether  $p(\delta(\mathbf{u})) \xrightarrow{\overline{T^* \cdot \overline{T_{\mathbf{J}}}} r(m)$  in  $\mathcal{W}$  for some  $m = d \cdot n \in S$ . This can be achieved by extending  $\mathcal{W}$  with a gadget that non deterministically subtracts some element of  $S$  after executing a transition from  $\overline{T_{\mathbf{J}}}$ . More precisely, since  $S$  is an (effectively) semilinear set of integers, it is also (effectively) ultimately periodic. Thus, it is possible to obtain a description of  $S = F \cup B + a \cdot \mathbb{N}$  where  $F = \{f_1, f_2, \dots, f_k\}$  and  $B = \{b_1, b_2, \dots, b_\ell\}$

are finite subsets of  $\mathbb{Z}$ . We extend  $\mathcal{W}$  with the gadget depicted in Figure 6. More precisely, for every transition  $t \in \overline{T_{\mathbf{J}}}$  leading to  $r$ , we add a new transition leading to a gadget that either subtracts some number from  $F$  or some number from  $B + a \cdot \mathbb{N}$ . Note that the gadget is not “attached” directly to  $r$  as we must ensure that  $r$  is entered by a transition of  $\overline{T_{\mathbf{J}}}$ . Hence, testing whether

$$p(\delta(\mathbf{u})) \xrightarrow{\overline{T^* \cdot \overline{T_{\mathbf{J}}}} r(m) \text{ in } \mathcal{W} \text{ for some } m \in S$$

amounts to testing whether  $p(\delta(\mathbf{u})) \xrightarrow{*} r'(0)$  in the new net. Since the latter can be done in polynomial space [FGH13], we are done.  $\square$

**7.2. Undecidability for monogenic classes.** In contrast with the previous result, we prove that decidability is undecidable in general for monogenic classes:

**Theorem 7.4.** *Reachability for monogenic affine  $\mathbb{Z}$ -VASS is undecidable. Moreover, there exists a fixed monogenic affine  $\mathbb{Z}$ -VASS for which deciding reachability is undecidable.*

We show the first part of Theorem 7.4 by giving a reduction from the problem of determining whether a given Diophantine equation has a solution over the natural numbers, which is well-known to be undecidable. The second part of Theorem 7.4 follows as a corollary. Indeed, by Matiyasevich’s theorem, Diophantine sets correspond to recursively enumerable sets. In particular, there exists a polynomial  $P$  such that

$$x \in \mathbb{N} \text{ is the encoding of a halting Turing machine } \iff \exists \mathbf{y} : P(x, \mathbf{y}) = 0.$$

The forthcoming construction will yield a monogenic affine  $\mathbb{Z}$ -VASS that can test “ $\exists \mathbf{y} : P(x, \mathbf{y}) = 0$ ” by nondeterministically guessing  $\mathbf{y}$  and testing  $P(x, \mathbf{y}) = 0$ . Hence, reachability cannot be decided for this monogenic affine  $\mathbb{Z}$ -VASS as the above language is undecidable.

Let us show the first part of Theorem 7.4. Let  $x_1, x_2, \dots, x_k$  be variables of a given polynomial  $P(x_1, x_2, \dots, x_k)$ . We will construct an instance of the reachability problem, for a monogenic affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$ , such that reachability holds if and only if  $P(x_1, x_2, \dots, x_k) = 0$  has a solution over  $\mathbb{N}^k$ .

The affine  $\mathbb{Z}$ -VASS will be described using the syntax of counter programs; see [Esp98, CLL<sup>+</sup>19], where a similar syntax was used to present the VASS model. We will make use of two instructions: **zero(x)?** and **loop**. The former checks whether counter  $x$  has value 0, and the latter repeats a block of instructions an arbitrary number of times. Figure 7 gives an example of such a program together with its translation as an affine  $\mathbb{Z}$ -VASS.

**Macros.** Before describing the reduction, let us introduce helpful macros. First, we define macros “**transfer x onto y**” and “**remove x from y**”. The former computes  $y = y + x$  and  $x = 0$ , and the latter computes  $y = y - x$  and  $x = 0$ . Both macros work under the assumption that  $x$  is initially non negative. These macros are implemented as follows:

$$\begin{array}{ll} \mathbf{transfer\ x\ onto\ y:} \ // \ \mathit{pre-cond.:} \ x \geq 0 & \mathbf{remove\ x\ from\ y:} \ // \ \mathit{pre-cond.:} \ x \geq 0 \\ \quad \mathbf{loop} & \quad \mathbf{loop} \\ \quad \quad x = x - 1 & \quad \quad x = x - 1 \\ \quad \quad y = y + 1 & \quad \quad y = y - 1 \\ \quad \mathbf{zero(x)?} & \quad \mathbf{zero(x)?} \end{array}$$

We define another macro “**t = square(s)**” for squaring the contents of a counter. More precisely, it computes  $s = t^2$  and  $t = 0$ . This macro is implemented as follows:

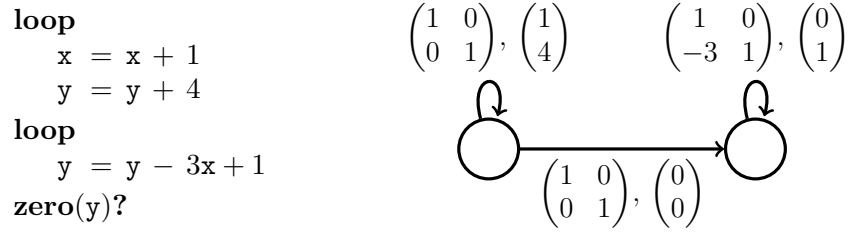


FIGURE 7. *Left*: an example program  $\mathcal{P}$  using instructions **zero?** and **loop**. *Right*: an affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$  equivalent to  $\mathcal{P}$ , where its first and second components correspond to counters  $x$  and  $y$  respectively. The program loops are simulated by loops within the control structure of  $\mathcal{V}$ . Note that whenever  $\mathcal{P}$  only adds and subtracts constants from counters, the associated matrix is the identity. Since the only way  $\mathcal{V}$  can test whether a counter equals 0 is at the end of the program via a reachability query, instruction **zero**( $y$ )? merely emphasizes that counter  $y$  will never be used again.

<pre> 1: t = <b>square</b>(s): 2:   <b>transfer s onto x</b> 3:   <b>loop</b> 4:     x = x - 1 5:     y = y + 1 6:     z = z + 2y + 1 7:   <b>zero</b>(x)? 8:   <b>transfer z onto t</b> 9:   <b>remove s from y</b> 10:  <b>zero</b>(y)? </pre>	<pre> // pre-condition: t = x = y = z = 0 // t = s^2, y = s and x = z = 0 // y = 0 </pre>
--	---

The above program starts with  $t$  and its auxiliary counters set to 0, and ends with  $s$  and the auxiliary counters set to 0. Its correctness follows by observing that  $(n+1)^2 = n^2 + (2n+1)$ .

We introduce one last macro “ $t = \mathbf{mult}(s, s')$ ” for multiplication. More precisely, it computes  $t = s \cdot s'$  and  $s = s' = 0$ . Its implementation exploits the fact that  $2mn = (m+n)^2 - m^2 - n^2$ :

<pre> t = <b>mult</b>(s, s'):   x = <b>square</b>(s)   y = <b>square</b>(s')   <b>transfer s onto z'</b>   <b>transfer s' onto z'</b>   z = <b>square</b>(z')   <b>remove x from z</b>   <b>remove y from z</b>   <b>loop</b>     z = z - 2     t = t + 1   <b>zero</b>(z)? </pre>	<pre> // pre-condition: t = x = y = z = z' = 0 // x = s^2 // y = (s')^2 // z = (s + s')^2, z' = 0 // z = 2 · s · s', x = y = 0 // t = s · s', z = 0 </pre>
--	--

The above program starts with  $\mathbf{t}$  and its auxiliary counters set to 0, and ends with  $\mathbf{s}$ ,  $\mathbf{s}'$  and its auxiliary counters set to 0. Note that a macro “ $\mathbf{t} = \mathbf{mult}(\mathbf{s}, c)$ ” for multiplying by a constant  $c$  can be achieved by a simpler program:

```

 $\mathbf{t} = \mathbf{mult}(\mathbf{s}, c):$                                 // pre-condition:  $\mathbf{t} = 0$ 
  loop
     $\mathbf{s} = \mathbf{s} - 1$ 
     $\mathbf{t} = \mathbf{t} + c$ 
  zero( $\mathbf{s}$ )?

```

Although these programs can be implemented rather straightforwardly by an affine  $\mathbb{Z}$ -VASS, two remarks are in order:

- Affine  $\mathbb{Z}$ -VASS do not have any native operation for testing a counter for zero. However, a counter  $\mathbf{x}$  can be tested *once* via a reachability query, provided that  $\mathbf{x}$  is left untouched after instruction **zero**( $\mathbf{x}$ )? has been invoked. Consequently, a *constant* number of zero-tests can be performed on a counter, provided its initial contents has been duplicated;
- Instruction “**transfer s onto t**” at line 2 of macro “ $\mathbf{t} = \mathbf{square}(\mathbf{s})$ ” destroys the contents of  $\mathbf{s}$  which is later needed at line 9. As for zero-tests, this is not an issue provided that some counter holds a copy of  $\mathbf{s}$ . Thus, only a *constant* number of squaring, and hence of multiplications, can be performed from a given counter.

**The construction.** Let us now describe the reachability instance. The initial vector is  $\mathbf{0}$ , which corresponds to having all counters set to 0 at the start of the program. The target vector is also  $\mathbf{0}$ , which corresponds to performing zero tests on all counters.

The program starts by performing a sequence of loops that guess a valuation  $\mathbf{x}$  for which  $P(\mathbf{x}) = 0$  is to be tested. More precisely, a value is nondeterministically picked for each variable  $x_i$  and stored in counters  $\mathbf{x}_i^1, \mathbf{x}_i^2, \dots, \mathbf{x}_i^{n_i}$ . The reason for having  $n_i$  copies of the value is to address the two issues mentioned earlier concerning zero-tests and reusing counters within macros. The precise number of copies,  $n_i$ , will be determined later. The fragment of code achieving the initialization is as follows:

```

loop
   $\mathbf{x}_1^1 = \mathbf{x}_1^1 + 1; \quad \mathbf{x}_1^2 = \mathbf{x}_1^2 + 1; \quad \dots \quad \mathbf{x}_1^{n_1} = \mathbf{x}_1^{n_1} + 1$ 
loop
   $\mathbf{x}_2^1 = \mathbf{x}_2^1 + 1; \quad \mathbf{x}_2^2 = \mathbf{x}_2^2 + 1; \quad \dots \quad \mathbf{x}_2^{n_2} = \mathbf{x}_2^{n_2} + 1$ 
   $\vdots$ 
loop
   $\mathbf{x}_k^1 = \mathbf{x}_k^1 + 1; \quad \mathbf{x}_k^2 = \mathbf{x}_k^2 + 1; \quad \dots \quad \mathbf{x}_k^{n_k} = \mathbf{x}_k^{n_k} + 1$ 

```

After the initialization, we compute the value of each monomial occurring within polynomial  $P(x_1, x_2, \dots, x_k)$ . This can be achieved using counters  $\mathbf{x}_i^j$  and the multiplication macro. Let  $Q(x_1, x_2, \dots, x_k)$  be a monomial of degree  $d$ . We show how to proceed by induction on  $d$ . If  $d = 0$ , then this is trivial. For larger degrees, we evaluate  $Q$  without its coefficient  $c$ , and then apply macro “ $\mathbf{t} = \mathbf{mult}(\mathbf{s}, c)$ ”. If  $d = 1$ , then we can simply transfer the appropriate counter  $\mathbf{x}_i^j$ . Otherwise,  $Q$  is a product of two monomials  $Q'$  and  $Q''$  of smaller degrees. By induction hypothesis, we can construct three copies of both monomials  $Q'$  and  $Q''$ . Then, using the multiplication macro, we obtain  $Q$ . Having evaluated all monomials, we can transfer each of their values to a common counter using the **transfer** and **remove**

macros depending on whether their sign is positive or negative. Finally, we test if the resulting value equals zero, which corresponds to having a solution to  $P(x_1, x_2, \dots, x_k) = 0$ .

Before arguing correctness of the construction, let us see why the whole program can be translated as a monogenic affine  $\mathbb{Z}$ -VASS  $\mathcal{V}$ , *i.e.* using only the identity matrix and one extra matrix  $\mathbf{A}$ . First, note that all macros have internal counters  $\mathbf{x}$ ,  $\mathbf{y}$  and  $\mathbf{z}$ . Every time we use a macro, we use three fresh counters, increasing the dimension of  $\mathcal{V}$ . Second, note that the only macro that requires a matrix different from the identity is “ $\mathbf{t} = \mathbf{square}(\mathbf{s})$ ”, which doubles  $\mathbf{y}$  during an assignment to  $\mathbf{z}$  at line 6. We will construct the matrix  $\mathbf{A}$  as follows. Suppose we want to encode one of the squaring macros. Matrix  $\mathbf{A}$  will have the same updates for all counters denoted as  $\mathbf{z}$  in all macros, but the vector will use constants according to this macro. That is, all coordinates for counters not occurring in this macro will be 0. In particular, counter  $\mathbf{z}$  from this macro will be updated like in line 6, *i.e.* “ $\mathbf{z} = \mathbf{z} + 2\mathbf{y} + 1$ ”, and all other counters corresponding to some other  $\mathbf{z}$  will be updated as “ $\mathbf{z} = \mathbf{z} + 2\mathbf{y}$ ”.

**Correctness.** We conclude by proving correctness of the construction. If  $P$  has a solution, then it is straightforward to extract a run from  $\mathcal{V}$ : (a) each  $\mathbf{x}_i^j$  is initialized according to the solution; and (b) each loop of the program is performed the exact number times so that each zero-test holds. It remains to observe that after performing a zero-test on some counter,  $\mathcal{V}$  does not perform any operation on this counter or performs “ $\mathbf{z} = \mathbf{z} + 2\mathbf{y}$ ”. But if the values of  $\mathbf{y}$  and  $\mathbf{z}$  are equal to zero, then  $\mathbf{z}$  will remain equal to zero after such an update.

Conversely, suppose there is a reachability witness (from  $\mathbf{0}$  to  $\mathbf{0}$ ). We claim that the initialization of counters  $\mathbf{x}_i^j$  provides a solution to  $P$ . To prove this, it suffices to show that every zero-test was valid. This is clear for all counters except for the  $\mathbf{z}$  within the squaring macro. Indeed, all other counters never change their values afterwards. However, counter  $\mathbf{z}$  is updated by “ $\mathbf{z} = \mathbf{z} + 2\mathbf{y}$ ”. If  $\mathbf{y}$  is non zero, then this will be detected by the zero-test on  $\mathbf{y}$ . Otherwise, the update “ $\mathbf{z} = \mathbf{z} + 2\mathbf{y}$ ” never changes the value of  $\mathbf{z}$  as required.

## 8. CONCLUSION

We have shown that the reachability problem for afmp- $\mathbb{Z}$ -VASS reduces to the reachability problem for  $\mathbb{Z}$ -VASS, *i.e.* every afmp- $\mathbb{Z}$ -VASS  $\mathcal{V}$  can be simulated by a  $\mathbb{Z}$ -VASS of size polynomial in  $|\mathcal{V}|$ ,  $|\mathcal{M}_{\mathcal{V}}|$  and  $\|\mathcal{M}_{\mathcal{V}}\|$ . In particular, this allowed us to establish that the reachability relation of any afmp- $\mathbb{Z}$ -VASS is semilinear.

For all nonnegative classes and consequently for all of the variants we studied — reset, permutation, transfer, copy and copyless  $\mathbb{Z}$ -VASS —  $|\mathcal{M}_{\mathcal{V}}|$  and  $\|\mathcal{M}_{\mathcal{V}}\|$  are of exponential size, thus yielding a PSPACE upper bound on their reachability problems. Moreover, we have established PSPACE-hardness for all of these specific classes, except for the reset case which is NP-complete.

We do not know whether an exponential bound on  $\|\mathcal{M}_{\mathcal{V}}\|$  holds for any class of afmp- $\mathbb{Z}$ -VASS over  $\mathbb{Z}^{d \times d}$ . We are aware that an exponential upper bound holds when  $\mathcal{M}_{\mathcal{V}}$  is generated by a single matrix [IS16]; and when  $\mathcal{M}_{\mathcal{V}}$  is a group then we have an exponential bound but only on  $|\mathcal{M}_{\mathcal{V}}|$  (see [KP02] for an exposition on the group case).

Finally, we have shown that there exists a (monogenic) class without the finite-monoid property for which reachability is decidable. This result was complemented by showing that reachability is undecidable in general for monogenic classes.

## ACKNOWLEDGMENTS

We are thankful to James Worrell for insightful discussions on transfer VASS.

## REFERENCES

- [ACJT96] Parosh Aziz Abdulla, Karlis Cerans, Bengt Jonsson, and Yih-Kuen Tsay. General decidability theorems for infinite-state systems. In *Proc. 11<sup>th</sup> Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 313–321, 1996.
- [AD16] Parosh Aziz Abdulla and Giorgio Delzanno. Parameterized verification. *International Journal on Software Tools for Technology Transfer*, 18(5):469–473, 2016.
- [AFR14] Rajeev Alur, Adam Freilich, and Mukund Raghothaman. Regular combinators for string transformations. In *Proc. Joint Meeting of the 23<sup>rd</sup> EACSL Annual Conference on Computer Science Logic (CSL) and the 29<sup>th</sup> ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 9:1–9:10, 2014.
- [AK76] Toshiro Araki and Tadao Kasami. Some decision problems related to the reachability problem for Petri nets. *Theoretical Computer Science*, 3(1):85–104, 1976.
- [ALW16] Konstantinos Athanasiou, Peizun Liu, and Thomas Wahl. Unbounded-thread program verification using thread-state equations. In *Proc. 8<sup>th</sup> International Joint Conference on Automated Reasoning (IJCAR)*, pages 516–531, 2016.
- [AR13] Rajeev Alur and Mukund Raghothaman. Decision problems for additive regular functions. In *Proc. 40<sup>th</sup> International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 37–48, 2013.
- [BFG<sup>+</sup>15] Michael Blondin, Alain Finkel, Stefan Göller, Christoph Haase, and Pierre McKenzie. Reachability in two-dimensional vector addition systems with states is PSPACE-complete. In *Proc. 30<sup>th</sup> Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 32–43, 2015.
- [BH17] Michael Blondin and Christoph Haase. Logics for continuous reachability in Petri nets and vector addition systems with states. In *Proc. 32<sup>nd</sup> Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12, 2017.
- [BHM18] Michael Blondin, Christoph Haase, and Filip Mazowiecki. Affine extensions of integer vector addition systems with states. In *Proc. 29<sup>th</sup> International Conference on Concurrency Theory (CONCUR)*, pages 14:1–14:17, 2018.
- [Boi98] Bernard Boigelot. *Symbolic Methods for Exploring Infinite State Spaces*. PhD thesis, Université de Liège, Belgium, 1998.
- [Bon13] Rémi Bonnet. *Theory of Well-Structured Transition Systems and Extended Vector-Addition Systems*. PhD thesis, École normale supérieure de Cachan, France, 2013.
- [CFM12] Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Bounded Parikh automata. *International Journal of Foundations of Computer Science*, 23(8):1691–1710, 2012.
- [CFM13] Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Unambiguous constrained automata. *International Journal of Foundations of Computer Science*, 24(7):1099–1116, 2013.
- [CH16] Dmitry Chistikov and Christoph Haase. The taming of the semi-linear set. In *Proc. 43<sup>rd</sup> International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 128:1–128:13, 2016.
- [CLL<sup>+</sup>19] Wojciech Czerwinski, Slawomir Lasota, Ranko Lazic, Jérôme Leroux, and Filip Mazowiecki. The reachability problem for petri nets is not elementary. In *Proc. 51<sup>st</sup> Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 24–33, 2019.
- [Del16] Giorgio Delzanno. A unified view of parameterized verification of abstract models of broadcast communication. *International Journal on Software Tools for Technology Transfer*, 18(5):475–493, 2016.
- [DFPS98] Catherine Dufourd, Alain Finkel, and Philippe Schnoebelen. Reset nets between decidability and undecidability. In *Proc. 25<sup>th</sup> International Colloquium on Automata, Languages and Programming (ICALP)*, pages 103–115, 1998.
- [ELM<sup>+</sup>14] Javier Esparza, Ruslán Ledesma-Garza, Rupak Majumdar, Philipp J. Meyer, and Filip Niksic. An SMT-based approach to coverability analysis. In *Proc. 26<sup>th</sup> International Conference on Computer Aided Verification (CAV)*, pages 603–619, 2014.



- [EN98] E. Allen Emerson and Kedar S. Namjoshi. On model checking for non-deterministic infinite-state systems. In *Proc. 13<sup>th</sup> Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 70–80, 1998.
- [Esp98] Javier Esparza. Decidability and complexity of Petri net problems — an introduction. In *Lectures on Petri Nets I*, pages 374–428, 1998.
- [FFSPS11] Diego Figueira, Santiago Figueira, Sylvain Schmitz, and Philippe Schnoebelen. Ackermannian and primitive-recursive bounds with Dickson’s lemma. In *Proc. 26<sup>th</sup> Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 269–278, 2011.
- [FGH13] Alain Finkel, Stefan Göller, and Christoph Haase. Reachability in register machines with polynomial updates. In *Proc. 38<sup>th</sup> International Symposium on Mathematical Foundations of Computer Science (MFCS)*, pages 409–420, 2013.
- [FL02] Alain Finkel and Jérôme Leroux. How to compose Presburger-accelerations: Applications to broadcast protocols. In *Proc. 22<sup>nd</sup> Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*, pages 145–156, 2002.
- [HH14] Christoph Haase and Simon Halfon. Integer vector addition systems with states. In *Proc. 8<sup>th</sup> International Workshop on Reachability Problems (RP)*, pages 112–124, 2014.
- [HP79] John E. Hopcroft and Jean-Jacques Pansiot. On the reachability problem for 5-dimensional vector addition systems. *Theoretical Computer Science*, 8:135–159, 1979.
- [HU79] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison-Wesley, 1979.
- [IS16] Radu Iosif and Arnaud Sangnier. How hard is it to verify flat affine counter systems with the finite monoid property? In *Proc. 14<sup>th</sup> International Symposium on Automated Technology for Verification and Analysis (ATVA)*, pages 89–105, 2016.
- [KKW14] Alexander Kaiser, Daniel Kroening, and Thomas Wahl. A widening approach to multithreaded program verification. *ACM Transactions on Programming Languages and Systems*, 36(4):14:1–14:29, 2014.
- [KM69] Richard M. Karp and Raymond E. Miller. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2):147–195, 1969.
- [Kos82] S. Rao Kosaraju. Decidability of reachability in vector addition systems (preliminary version). In *Proc. 14<sup>th</sup> Annual ACM Symposium on Theory of Computing (STOC)*, pages 267–281, 1982.
- [KP02] James Kuzmanovich and Andrey Pavlichenkov. Finite groups of matrices whose entries are integers. *The American Mathematical Monthly*, 109(2):173–186, 2002.
- [Ler12] Jérôme Leroux. Vector addition systems reachability problem (a simpler solution). In *The Alan Turing Centenary Conference*, pages 214–228, 2012.
- [Lip76] Richard J. Lipton. The reachability problem requires exponential space. Technical Report 63, Department of Computer Science, Yale University, 1976.
- [May84] Ernst W. Mayr. An algorithm for the general Petri net reachability problem. *SIAM Journal on Computing*, 13(3):441–460, 1984.
- [Min67] Marvin Lee Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall, 1967.
- [MS77] Arnaldo Mandel and Imre Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, 1977.
- [Pre29] Mojżesz Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Comptes Rendus du I<sup>er</sup> Congrès des mathématiciens des pays slaves*, pages 192–201, 1929.
- [Rac78] Charles Rackoff. The covering and boundedness problems for vector addition systems. *Theoretical Computer Science*, 6:223–231, 1978.
- [Rei08] Klaus Reinhardt. Reachability in Petri nets with inhibitor arcs. *Electronic Notes in Theoretical Computer Science*, 223:239–264, 2008.
- [Rei15] Julien Reichert. *Reachability games with counters: decidability and algorithms*. PhD thesis, École normale supérieure de Cachan, France, 2015.
- [Sch10] Philippe Schnoebelen. Revisiting Ackermann-hardness for lossy counter machines and reset Petri nets. In *Proc. 35<sup>th</sup> International Symposium Mathematical Foundations of Computer Science (MFCS)*, pages 616–628, 2010.
- [Web87] Andreas Weber. *Über die Mehrdeutigkeit und Wertigkeit von endlichen Automaten und Transducern*. PhD thesis, Goethe-Universität Frankfurt am Main, 1987.

- [WS91] Andreas Weber and Helmut Seidl. On finitely generated monoids of matrices with entries in  $\mathbb{N}$ . *Informatique Théorique et Applications*, 25:19–38, 1991.