Termination of linear loops under commutative updates

Ruiwen Dong
ruiwen.dong@kellogg.ox.ac.uk
University of Oxford
Oxford, United Kingdom

ABSTRACT

We consider the following problem: given $d \times d$ rational matrices $A_1, \ldots, A_k$ and a polyhedral cone $C \subset \mathbb{R}^d$, decide whether there exists a non-zero vector whose orbit under multiplication by $A_1, \ldots, A_k$ is contained in C. This problem can be interpreted as verifying the termination of multi-path while loops with linear updates and linear guard conditions. We show that this problem is decidable for *commuting* invertible matrices $A_1, \ldots, A_k$. The key to our decision procedure is to reinterpret this problem in a purely algebraic manner. Namely, we discover its connection with modules over the polynomial ring $\mathbb{R}[X_1, \ldots, X_k]$ as well as the polynomial semiring $\mathbb{R}_{\geq 0}[X_1, \ldots, X_k]$. The loop termination problem is then reduced to deciding whether a submodule of $(\mathbb{R}[X_1, \ldots, X_k])^n$ contains a "positive" element.

KEYWORDS

loop termination, commuting matrices, positive polynomials, module over polynomial ring

1 INTRODUCTION

We consider the termination problem for multipath (or branching) linear loops over the real numbers. We are concerned with problems of the following form: given $d \times d$ matrices $A_1, \ldots, A_k$ and a subset C of $\mathbb{R}^d$, decide whether there exists a vector $v \in C$ whose orbit under multiplication by $A_1, \ldots, A_k$ is contained in C. In other words, denote by $\langle A_1, \ldots, A_k \rangle$ the monoid generated by $A_1, \ldots, A_k$, we want to decide whether there exists $v \in C$ such that $Av \in C$ for all $A \in \langle A_1, \ldots, A_k \rangle$. Such a problem can be interpreted as the non-termination of the following linear loop:

$$\text{while } x \in C \text{ do } (x := A_1 x \text{ or } \cdots \text{ or } x := A_k x). \qquad (1)$$

The problem is whether there exists an initial value v such that the loop never terminates. Analysis of loops of this form is an important part of analysing more complex programs [10, 11]. Various tools such as computing polynomial invariants [9], porous invariants [12], ranking functions [3, 4] have been developed to analyse properties of such multipath loops.

Termination of linear loops with a *single* update ($k = 1$) has been intensely studied for the last twenty years. Tiwari [16] first showed its decidability in the case where the guard condition C is a convex polyhedron. Subsequently, Braverman [6] extended the decidability result to the case where C is the set of rational points in a convex polyhedron; and Hosseini, Ouaknine, Worrell [8] further extended the result to integer points.[1]

In the above results, the decidability relies on the freedom of choosing the initial value v to circumvent the difficulties inherent in deciding termination on a single initial value. In fact, when C is a closed halfspace, termination of single-path linear loops for a *fixed* initial value, that is,

$$x := v; \text{ while } x \in C \text{ do } (x := Ax), \qquad (2)$$

subsumes the *Positivity Problem* [14]. The Positivity Problem at dimension greater than five has been shown to be intrinsically hard; and its decidability would entail major breakthroughs in open problems in Diophantine approximation [14]. Therefore, the freedom of choice for the initial value is crucial in proving decidability results.

In this paper we consider termination of the multipath loop (1) under *commutative* updates, that is, when $A_1, \ldots, A_k$ are commuting matrices. In [1], Babai, Beals, Cai, Ivanyos and Luks proved various results on reachability problems of multipath linear loops under commutative updates. A continuous analogue of the reachability problem has been studied in [13]. For the termination problem, we restrict to the case where C is a *polyhedral cone*, that is,

$$C := \left\{ x \in \mathbb{R}^d \;\middle|\; c_i^\top x \geq 0, i = 1, \ldots, n \right\}$$

for some $c_1, \ldots, c_n \in \mathbb{R}^d$. We will also exclude the initial value $(0, \ldots, 0)$ since it is trivially invariant under linear updates. For the sake of simplicity, we will suppose $A_1, \ldots, A_k$ to have rational entries and are invertible, and that $c_1, \ldots, c_n \in \mathbb{Q}^d$. Our main result (see Theorem 5) is that termination of such multipath linear loops is decidable.

If one tries to adapt the proofs for the single update case to multiple updates, natural attempts will start by simultaneously diagonalizing the update matrices and analysing their actions on the

---

[1]The original results all concern single *affine* updates. However, they are equivalent to the case of *linear* updates by increasing the dimension by one and homogenizing the coordinates.

cone geometrically. Unfortunately such analysis depends on classifying the complex eigenvalues of all the update matrices. Besides the unavoidable tedious case analysis, it is also not clear how to circumvent certain problems related to Diophantine approximation, as such circumvention appears ad hoc in the single update case. Our main contribution is a completely algebraic approach that overcomes this difficulty. In particular, using the duality of linear programming, we reduce the problem to deciding whether an orbit cone is *salient*. We show that deciding whether an orbit is salient is equivalent to deciding whether a submodule of $(\mathbb{R}[X_1, \ldots, X_k])^n$ contains an element with only positive coefficients. We then use a result of Einsiedler, Mouat, and Tuncel [7] and the decidability of first order theory of the reals to deduce the desired result.

2 PRELIMINARIES

2.1 Convex geometry

A *convex cone* in $\mathbb{R}^d$ is a subset $C \subset \mathbb{R}^d$ that satisfies $r \in \mathbb{R}_{\geq 0}, v \in C \implies r \cdot v \in C$ and $v, w \in C \implies v + w \in C$. In this article, we will use the word *cone* to imply convex cones. A *polyhedral* cone is a cone of the form

$$C := \left\{ x \in \mathbb{R}^d \ \middle| \ c_i^\top x \geq 0, i = 1, \ldots, n \right\}.$$

for finitely many given non-zero vectors $c_1, \ldots, c_n \in \mathbb{R}^d$.

Given mutually commuting matrices $A_1, \ldots, A_k \in \mathbb{R}^{d \times d}$, and a vector $v \in \mathbb{R}^d$, denote by

$$\langle A_1, \ldots, A_k \rangle \cdot v := \left\{ A_1^{n_1} \cdots A_k^{n_k} v \ \middle| \ n_1, \ldots, n_k \in \mathbb{N} \right\}$$

the orbit of v under multiplication by $A_1, \ldots, A_k$. Similarly, given a cone $C \subset \mathbb{R}^d$, denote by

$$\langle A_1, \ldots, A_k \rangle \cdot C := \left\{ A_1^{n_1} \cdots A_k^{n_k} v \ \middle| \ n_1, \ldots, n_k \in \mathbb{N}, v \in C \right\}$$

the orbit of C under multiplication by $A_1, \ldots, A_k$.

Given an arbitrary subset $S \subset \mathbb{R}^d$, denote by $cone(S)$ the smallest cone in $\mathbb{R}^d$ containing S. Similarly, denote by $lin(S)$ the smallest linear space in $\mathbb{R}^d$ containing S.

A *closed halfspace* of a $\mathbb{R}^d$ is a subset $\mathcal{H}$ defined by $\mathcal{H} := \{ x \mid v^\top x \geq 0 \}$ for some $v \in \mathbb{R}^d \setminus \{0^d\}$. Here, 0^d denotes the zero vector of $\mathbb{R}^d$. By the Supporting Hyperplane Theorem [5, Chapter 2.5.2] (applied at the point 0^d), every cone $C \subset \mathbb{R}^d$ is either contained in some closed halfspace or it is $\mathbb{R}^d$ itself.

A cone C is called *salient* if $C \cap -C = \{0^d\}$, where $-C := \{-v \mid v \in C\}$. An arbitrary set $S \subset \mathbb{R}^d$ is called salient if $cone(S)$ is salient. Obviously every salient cone (and hence every salient set) is contained in a closed halfspace because a salient cone cannot be $\mathbb{R}^d$.

2.2 Modules over polynomial rings

Fix an integer $k \geq 1$. In this paper we consider the polynomial ring $\mathbb{A} := \mathbb{R}[X_1, \ldots, X_k]$ and its sub-semiring

$$\mathbb{A}^+ = \mathbb{R}_{\geq 0}[X_1, \ldots, X_k]$$

$$:= \left\{ \sum_{n_1, \ldots, n_k \in \mathbb{N}} r_{n_1, \ldots, n_k} X_1^{n_1} \cdots X_k^{n_k} \ \middle| \ r_{n_1, \ldots, n_k} \in \mathbb{R}_{\geq 0}, \right.$$

$$\left. r_{n_1, \ldots, n_k} = 0 \text{ for all but finitely many } r_{n_1, \ldots, n_k} \right\}.$$

That is, $\mathbb{A}^+ \subset \mathbb{A}$ is the sub-semiring of polynomials with non-negative coefficients. Define additionally $\mathbb{A}^{++} := \mathbb{A}^+ \setminus \{0\}$.

Let $\mathbb{A}^n := \{(f_1, \ldots, f_n) \mid f_1, \ldots, f_n \in \mathbb{A}\}$. An $\mathbb{A}$-*submodule* of $\mathbb{A}^n$ is a subset $\mathcal{M} \subset \mathbb{A}^n$ such that $v, w \in \mathcal{M} \implies v + w \in \mathcal{M}$ and $f \in \mathbb{A}, v \in \mathcal{M} \implies f \cdot v \in \mathcal{M}$. Here $f \cdot (f_1, \ldots, f_n) := (ff_1, \ldots, ff_n)$.

For example, given $g_1, \ldots, g_m \in \mathbb{A}^n$, the set

$$\mathcal{M} = g_1 \mathbb{A} + \cdots + g_m \mathbb{A}$$

$$:= \{ f_1 \cdot g_1 + \cdots + f_m \cdot g_m \mid f_1, \ldots, f_m \in \mathbb{A} \}$$

is an $\mathbb{A}$-submodule of $\mathbb{A}^n$. In this case we will say that $g_1, \ldots, g_m$ form a *basis* of $\mathcal{M}$. The above definition still works when one replaces $\mathbb{A}$ by any commutative ring.

Naturally, we define the following subset of $\mathbb{A}^n$:

$$\left(\mathbb{A}^+ \right)^n := \{ (f_1, \ldots, f_n) \mid f_1, \ldots, f_n \in \mathbb{A}^+ \}.$$

The key ingredient of our paper is a deep result by Einsiedler, Mouat, and Tuncel [7] that characterizes when an $\mathbb{A}$-submodule of $\mathbb{A}^n$ contains an element of $\left(\mathbb{A}^+ \right)^n \setminus \{0^n\}$. We will state this result in Section 6.

3 OVERVIEW OF THE DECISION PROCEDURE

In this section we give an overview of the procedure that decides (non-)termination of the multipath loops under commutative updates. In rigorous terms, given commuting matrices $A_1, \ldots, A_k$ and a polyhedral cone C, we want to decide whether there exists a vector $v \in \mathbb{R}^d \setminus \{0^d\}$, such that $\langle A_1, \ldots, A_k \rangle \cdot v \subset C$.

Let the cone C be given by

$$C := \left\{ x \in \mathbb{R}^d \ \middle| \ c_i^\top x \geq 0, i = 1, \ldots, n \right\}. \tag{3}$$

We define its *dual cone* C^* as

$$C^* := \left\{ x \in \mathbb{R}^d \ \middle| \ x = r_1 c_1 + \cdots + r_n c_n, r_1, \ldots, r_n \in \mathbb{R}_{\geq 0} \right\}. \tag{4}$$

Our first lemma is a duality type argument that reduces the termination problem to deciding whether an orbit is contained in some halfspace.

LEMMA 1. *The following two conditions are equivalent:*

(i) There exists $v \in \mathbb{R}^d \setminus \{0^d\}$, such that $\langle A_1, \ldots, A_k \rangle \cdot v \subset C$.
(ii) The orbit $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is contained in a closed halfspace.

The proof of Lemma 1 is given in Section 4. Deciding whether an orbit has the property of being contained in a closed halfspace is challenging. In particular, the smallest cone containing the orbit might not be finitely generated. It is very unlikely that one can compute any precise description of this cone, otherwise one would be able to decide whether it is contained in a *given* halfspace, and

hence solve the Positivity Problem, entailing breakthroughs in number theory [14]. Therefore, we will first devise a procedure that decides a similar property for the orbit, namely whether it is salient. We will later use it as a sub-procedure to decide whether the orbit is contained in a closed halfspace. The next lemma reduces deciding salient-ness to finding certain tuples of polynomials in $\mathbb{A}^+$.

LEMMA 2. *The following two conditions are equivalent:*
(i) *The orbit* $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ *is not salient.*
(ii) *There exists a tuple of polynomials* $(f_1, \ldots, f_n) \in \left(\mathbb{A}^+\right)^n \setminus \{0^n\}$, *not all zero, such that* $\sum_{i=1}^n f_i(A_1^\top, \ldots, A_k^\top) \cdot c_i = 0^d$.

The proof of Lemma 2 is given in Section 4.
Define the following $\mathbb{A}$-submodule of $\mathbb{A}^n$.

$$ \mathcal{M} := \left\{ (f_1, \ldots, f_n) \in \mathbb{A}^n \ \middle| \ \sum_{i=1}^n f_i(A_1^\top, \ldots, A_k^\top) \cdot c_i = \mathbf{0} \right\}. \quad (5) $$

One easily verifies that $g, h \in \mathcal{M} \implies g + h \in \mathcal{M}$, as well as $f \in \mathbb{A}, g \in \mathcal{M} \implies f \cdot g \in \mathcal{M}$; so $\mathcal{M}$ is indeed an $\mathbb{A}$-module. Observe that condition (ii) of Lemma 2 can be expressed as "$\mathcal{M}$ contains an element of $\left(\mathbb{A}^+\right)^n \setminus \{0^d\}^n$". The next proposition shows that a basis of $\mathcal{M}$ is computable.

PROPOSITION 3. *Given as input* $A_1, \ldots, A_k$ *and* $c_1, \ldots, c_n$, *one can compute a basis* $g_1, \ldots, g_m \in \mathbb{A}^n$ *such that* $\mathcal{M} = g_1 \mathbb{A} + \cdots + g_m \mathbb{A}$.

The proof of Proposition 3 is given in Section 5. The next proposition shows that it is decidable whether the module $\mathcal{M}$ contains an element of $\left(\mathbb{A}^+\right)^n \setminus \{0^n\}$. Hence condition (ii) of Lemma 2 is decidable.

PROPOSITION 4. *There is a procedure that, given as input a basis* $g_1, \ldots, g_m \in \mathbb{A}^n$ *with rational coefficients such that* $\mathcal{M} = g_1 \mathbb{A} + \cdots + g_m \mathbb{A}$, *decides whether* $\mathcal{M}$ *contains an element of* $\left(\mathbb{A}^+\right)^n \setminus \{0^n\}$, *and outputs this element* f *in case it exists.*

The proof of Proposition 4 is given in Section 6. Combining Lemma 2, Proposition 3 and 4, we conclude that it is decidable whether the orbit $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is salient. We now use this to show that it is decidable whether $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is contained in a closed halfspace. This together with Lemma 1 will give us the main result:

THEOREM 5. *Given commuting invertible matrices* $A_1, \ldots, A_k \in \mathbb{Q}^{d \times d}$ *and vectors* $c_1, \ldots, c_n \in \mathbb{Q}^d$ *defining a polyhedral cone* C *as in Equation* (3), *it is decidable whether there exists* $v \in \mathbb{R}^d \setminus \{0^d\}$ *such that* $\langle A_1, \ldots, A_k \rangle \cdot v \subset C$.

PROOF. By Lemma 1, it suffices to construct a procedure that decides whether the orbit $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is contained in a closed halfspace. We use induction on d. When $d = 1$, the decision procedure is easy: $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is contained in a closed halfspace if and only if $c_1, \ldots, c_n$ all have the same sign and $A_1, \ldots, A_k$ are all positive rationals.

Suppose we have a decision procedure for all dimensions smaller than d, we now construct a procedure for dimension d. By Lemma 2, Proposition 3 and 4, it is decidable whether the orbit $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is salient.

If the orbit is salient, then it is contained in some closed halfspace. If the orbit is not salient, then $\mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$ contains

the vectors w and $-w$ for some $w \in \mathbb{R}^d \setminus \{0^d\}$. Such a w can be effectively computed in the following way: by Proposition 4, one can compute an element $f \in \mathcal{M} \cap \left(\mathbb{A}^+\right)^n \setminus \{0^n\}$. Then, as in the proof of Lemma 2 (see Section 4), one can obtain from f a non-zero vector $w \in \mathbb{Q}^d$ such that $\pm w \in \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$.

We then compute (a basis of) the linear space

$$ W := \mathbf{lin}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot w\right). $$

This can be done by starting with $W := \mathbb{R}w$ and repeatedly replacing W by $W + A_1 W + \cdots + A_k W$ until $W = W + A_1 W + \cdots + A_k W$. This process must terminate since the dimension of W is always growing. The resulting $W = \mathbf{lin}\left(\langle A_1^\top, \ldots, A_k^\top \rangle w\right)$ is invariant under the linear maps $A_1^\top, \ldots, A_k^\top$. Since $\mathbb{R}w \subset \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$ we have $W \subset \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$.

The quotient $\mathbb{R}^d / W$ is isomorphic to $\mathbb{R}^{d - \dim(W)}$ after fixing a basis. We can suppose this basis admits only rational entries. Composing with the canonical map $\mathbb{R}^d \to \mathbb{R}^d / W$ we have an (effectively computable) map

$$ \pi \colon \mathbb{R}^d \longrightarrow \mathbb{R}^{d - \dim(W)} $$

with $\ker(\pi) = W$. Since multiplication by the matrices $A_1^\top, \ldots, A_k^\top$ leaves W invariant, these matrices act on $\mathbb{R}^d / W \cong \mathbb{R}^{d - \dim(W)}$ linearly. We denote these actions by

$$ B_1, \ldots, B_k \in \mathbb{Q}^{(d - \dim(W)) \times (d - \dim(W))}. $$

These matrices are obviously invertible, commuting and effectively computable.

Using the induction hypothesis on the dimension d, we can decide whether the image

$$ \pi\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right) = \langle B_1, \ldots, B_k \rangle \cdot \pi(C^*) $$

is contained in some closed halfspace (of $\mathbb{R}^d / W \cong \mathbb{R}^{d - \dim(W)}$). If the image $\pi\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$ is contained in a closed halfspace $\mathcal{H} \subset \mathbb{R}^{d - \dim(W)}$ then $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is contained in the closed halfspace $\pi^{-1}(\mathcal{H}) \subset \mathbb{R}^d$. Otherwise,

$$ \mathbf{cone}\left(\pi\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)\right) = \mathbb{R}^{d - \dim(W)}. $$

Since $\pi(v + w) = \pi(v) + \pi(w)$ for all $v, w \in \mathbb{R}^d$, the above equation yields

$$ \pi\left(\mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)\right) = \mathbb{R}^{d - \dim(W)}. $$

Thus, any $v \in \mathbb{R}^d$ can be written as $v' + v''$ where

$$ v' \in \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right), $$

and $v'' \in W$. Recall that $W \subset \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$. Therefore, $v = v' + v'' \in \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$ for all $v \in \mathbb{R}^d$. So

$$ \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right) = \mathbb{R}^d $$

is not contained in any closed halfspace. □

4 FROM LINEAR LOOPS TO POSITIVE POLYNOMIALS

In this section we give the proofs of Lemma 1 and 2.

PROOF OF LEMMA 1. (i) $\implies$ (ii). Suppose $v \in \mathbb{R}^d \setminus \{0^d\}$, such that $\langle A_1, \ldots, A_k \rangle \cdot v \subset C$. Then by the definition of C, for all $n_1, \ldots, n_k \in \mathbb{N}$ and $i = 1, \ldots, n$, we have $c_i^\top A_1^{n_1} \cdots A_k^{n_k} v \geq 0$. Taking the transpose yields

$$v^\top \left(A_k^\top\right)^{n_k} \cdots \left(A_1^\top\right)^{n_1} c_i \geq 0, \quad i = 1, \ldots, n; n_1, \ldots, n_k \in \mathbb{N}. \quad (6)$$

Let $\mathcal{H}$ be the closed halfspace defined by $\mathcal{H} := \{x \in \mathbb{R}^d \mid v^\top x \geq 0\}$. Then Equation (6) shows that $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot c_i \subset \mathcal{H}$ for all i. Since the cone C^* is generated by $c_1, \ldots, c_n$, we have $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^* \subset \mathcal{H}$.

(ii) $\implies$ (i). Suppose $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is contained in the halfspace $\mathcal{H}$ defined by $\mathcal{H} := \{x \in \mathbb{R}^d \mid v^\top x \geq 0\}$, where $v \neq 0^d$. Then Equation (6) holds for all i and all $n_1, \ldots, n_k \in \mathbb{N}$. Taking the transpose yields $c_i^\top A_1^{n_1} \cdots A_k^{n_k} v \geq 0$ and hence $\langle A_1, \ldots, A_k \rangle \cdot v \subset C$. □

PROOF OF LEMMA 2. (i) $\implies$ (ii). If $\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ is not salient, then there exists $v \neq 0^d$ with $v, -v \in \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$. Therefore, there exist finitely many positive reals $r_{i,n_1,\ldots,n_k}$, such that

$$\sum_{i=1}^n \sum_{n_1,\ldots,n_k \in \mathbb{N}} r_{i,n_1,\ldots,n_k} \left(A_1^\top\right)^{n_1} \cdots \left(A_k^\top\right)^{n_k} \cdot c_i = v.$$

In order words, there exist polynomials with non-negative coefficients $(g_1, \ldots, g_n) \in (\mathbb{A}^+)^n$, such that $\sum_{i=1}^n g_i(A_1^\top, \ldots, A_k^\top) \cdot c_i = v$. Similarly, there exist polynomials $(h_1, \ldots, h_n) \in (\mathbb{A}^+)^n$, such that $\sum_{i=1}^n h_i(A_1^\top, \ldots, A_k^\top) \cdot c_i = -v$. Since $v \neq 0^d$, we know that $g_1, \ldots, g_n$ are not all zero. Let $f_i := g_i + h_i, i = 1, \ldots, n$, then $\sum_{i=1}^n f_i(A_1^\top, \ldots, A_k^\top) \cdot c_i = 0^d$; and $(f_1, \ldots, f_n) \in (\mathbb{A}^+)^n \setminus \{0^n\}$.

(ii) $\implies$ (i). Suppose $\sum_{i=1}^n f_i(A_1^\top, \ldots, A_k^\top) \cdot c_i = 0^d$ for some $(f_1, \ldots, f_n) \in (\mathbb{A}^+)^n \setminus \{0^n\}$. Without loss of generality suppose $f_1 \neq 0$. Let g be a monomial of f_1 and write $f_1 = g + f_1'$. Since $f_1 \in \mathbb{A}^+$, we have also $g, f_1' \in \mathbb{A}^+$. We have $v := g(A_1^\top, \ldots, A_k^\top) \cdot c_1 \neq 0^d$ because $A_1^\top, \ldots, A_k^\top$ are invertible, $c_1 \neq 0^d$ and because g is a monomial. Then $v = g(A_1^\top, \ldots, A_k^\top) \cdot c_1 \in \langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*$ and

$$-v = f_1'(A_1^\top, \ldots, A_k^\top) \cdot c_1 + \sum_{i=2}^n f_i(A_1^\top, \ldots, A_k^\top) \cdot c_i$$
$$\in \mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right).$$

Thus, $\mathbf{cone}\left(\langle A_1^\top, \ldots, A_k^\top \rangle \cdot C^*\right)$ contains both v and $-v$ and is therefore not salient. □

5 COMPUTING THE MODULE $\mathcal{M}$

In this section we prove Proposition 3. Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{A}^n$, that is,

$$e_i = (0, \cdots, 0, 1, 0, \cdots, 0),$$

where the i-th coordinate is one.

The vector space $\mathbb{R}^d$ can be considered as an $\mathbb{A}$-module by $f \cdot v := f(A_1^\top, \ldots, A_k^\top)v$ for all $f \in \mathbb{A}, v \in \mathbb{R}^d$. Define the following map of $\mathbb{A}$-modules:

$$\varphi : \mathbb{A}^n \longrightarrow \mathbb{R}^d, \quad (7)$$

$$\sum_{i=1}^n f_i e_i \mapsto \sum_{i=1}^n f_i(A_1^\top, \ldots, A_k^\top) c_i. \quad (8)$$

Then the $\mathbb{A}$-module $\mathcal{M}$ defined in (5) is exactly $\ker(\varphi)$.

PROOF OF PROPOSITION 3. Let $F_1 \in \mathbb{R}[X_1], \ldots, F_k \in \mathbb{R}[X_k]$ be the (monic) characteristic polynomials of $A_1^\top, \ldots, A_k^\top$, respectively. Then $F_j(A_j^\top) = 0^{d \times d}$, so obviously $F_j e_i \in \mathcal{M}$ for all $1 \leq j \leq k, 1 \leq i \leq n$. Define the (finite) set of monomials

$$S := \{X_1^{n_1} \cdots X_k^{n_k} e_i \mid n_1 < \deg F_1, \ldots, n_k < \deg F_k, 1 \leq i \leq n\}.$$

Consider the map

$$\lambda : \mathbb{R}^{\mathrm{card}(S)} \longrightarrow \mathbb{R}^d, \quad (9)$$

$$(r_s)_{s \in S} \mapsto \sum_{s \in S} r_s \varphi(s). \quad (10)$$

One can effectively compute a basis $(r_{1s})_{s \in S}, \ldots, (r_{ps})_{s \in S}$ of $\ker(\lambda)$. Define the set

$$\mathcal{R} := \left\{ \sum_{s \in S} r_{js} \cdot s \ \middle| \ j = 1, \ldots, p \right\}$$

of elements in $\mathbb{A}^n$. Clearly $\mathcal{R} \subset \ker(\varphi) = \mathcal{M}$. Define additionally the following subset of $\mathcal{M}$:

$$\mathcal{F} := \left\{ F_j e_i \ \middle| \ 1 \leq j \leq k, 1 \leq i \leq n \right\}.$$

We claim that $\mathcal{R} \cup \mathcal{F}$ is a basis for $\mathcal{M}$.

To prove this claim, let L be the $\mathbb{A}$-module generated by $\mathcal{R} \cup \mathcal{F}$. It is a submodule of $\mathcal{M}$. We will show $L = \mathcal{M}$. Let $f = \sum_{i=1}^n f_i e_i$ be an element of $\mathcal{M}$.

Every monomial $m := X_1^{n_1} \cdots X_k^{n_k}$ of every polynomial $f_i, i = 1, \ldots, n$, can be written as two polynomials $m = p' + p''$ such that $p'' e_i \in L$ and every monomial of $p' e_i$ is in the set S. Indeed, denote $J := \{1 \leq j \leq k \mid n_j > \deg F_j\}$. We write $J = \{i_1, \ldots, i_d\}$ for some $d \leq k$, and where $i_1, \ldots, i_d, i_{d+1}, \ldots, i_k$ is some permutation of $(1, \ldots, k)$. We divide $X_j^{n_j}$ by F_j for every $j \in J$ and obtain

$$X_j^{n_j} = P_j F_j + R_j,$$

with $\deg R_j < \deg F_j$. Then

$$m - (P_{i_1} F_{i_1}) X_{i_2}^{n_{i_2}} \cdots X_{i_k}^{n_{i_k}} = R_{i_1} X_{i_2}^{n_{i_2}} \cdots X_{i_k}^{n_{i_k}},$$

with $(P_{i_1} F_{i_1}) X_{i_2}^{n_{i_2}} \cdots X_{i_k}^{n_{i_k}} e_i \in L$, and

$$R_{i_1} X_{i_2}^{n_{i_2}} \cdots X_{i_k}^{n_{i_k}} - R_{i_1}(P_{i_2} F_{i_2}) X_{i_3}^{n_{i_3}} \cdots X_{i_k}^{n_{i_k}} = R_{i_1} R_{i_2} X_{i_3}^{n_{i_3}} \cdots X_{i_k}^{n_{i_k}},$$

with $R_{i_1}(P_{i_2} F_{i_2}) X_{i_3}^{n_{i_3}} \cdots X_{i_k}^{n_{i_k}} e_i \in L$. Continue this process until i_d, we obtain $m = p' + p''$ where

$$p' = R_{i_1} \cdots R_{i_d} X_{i_{d+1}}^{n_{i_{d+1}}} \cdots X_{i_k}^{n_{i_k}},$$

and

$$p'' = (P_{i_1} F_{i_1}) X_{i_2}^{n_{i_2}} \cdots X_{i_k}^{n_{i_k}} + R_{i_1}(P_{i_2} F_{i_2}) X_{i_3}^{n_{i_3}} \cdots X_{i_k}^{n_{i_k}} + \cdots + R_{i_1} \cdots R_{i_{d-1}}(P_{i_d} F_{i_d}) X_{i_{d+1}}^{n_{i_{d+1}}} \cdots X_{i_k}^{n_{i_k}}.$$

Clearly, every monomials of p' is in the set $\mathcal{S}$, and $p'' e_i \in L$.

Decompose every monomial of every $f_i, i = 1, \ldots, n$. In this way, f can be written as $f = f' + f''$ with $f'' \in L$, and f' containing only monomials from the set $\mathcal{S}$. Since $f'' \in L \subseteq \mathcal{M}$ and $f \in \mathcal{M}$, we have $f' \in \mathcal{M}$. We claim that f' is generated as an $\mathbb{A}$-module by the set $\mathcal{R}$. Write $f' = \sum_{s \in S} f_s \cdot s$. Since $f' \in \mathcal{M}$, we have $\sum_{s \in S} f_s \varphi(s) = \varphi(f') = 0^d$, hence $(f_s)_{s \in S} \in \ker(\lambda)$. Therefore the vector $(f_s)_{s \in S} \in \mathbb{R}^S$ can be written as $\mathbb{R}$-linear combination of the basis $(r_{1s})_{s \in S}, \ldots, (r_{ps})_{s \in S}$. Thus, $f' = \sum_{s \in S} f_s \cdot s$ can also be written as a $\mathbb{R}$-linear combination of the elements $\sum_{s \in S} r_{1s} \cdot s, \ldots, \sum_{s \in S} r_{ps} \cdot s$ in $\mathbb{A}^n$. This shows that f' is in the $\mathbb{R}$-module generated by $\mathcal{R}$. A fortiori, it is in the $\mathbb{A}$-module generated by $\mathcal{R}$. Therefore, $f = f' + f''$ is in L.

We have thus found the finite basis $\mathcal{R} \cup \mathcal{F}$ for $\mathcal{M}$ as an $\mathbb{A}$-module. Note that the procedure described in the proof is effective: the computation of the characteristic polynomials $F_1, \ldots, F_k$ can be done by computing the determinants $\det(A_i - XI), i = 1, \ldots, k$, and the computation of $\ker(\lambda)$ is simply linear algebra. □

Note that since the entries of the matrices $A_1, \ldots, A_k$ and the vectors $c_1, \ldots, c_n$ are all rationals, the computation given in Proposition 3 can be done over the rational. Hence, we can suppose the computed basis of $\mathcal{M}$ has rational coefficients.

6 POSITIVE POLYNOMIAL MEMBERSHIP

In this section we prove Proposition 4. Recall $\mathbb{A}^{++} := \mathbb{A}^+ \setminus \{0\}$. Let $\mathbb{B} := \mathbb{R}[X_1^{\pm 1}, \ldots, X_k^{\pm 1}]$ be the Laurent polynomial ring over k variables, and $\mathbb{B}^+ := \mathbb{R}_{\geq 0}[X_1^{\pm 1}, \ldots, X_k^{\pm 1}]$ be the sub-semiring of Laurent polynomials with non-negative coefficients. Define $\mathbb{B}^{++} := \mathbb{B}^+ \setminus \{0\}$.

The first step to proving Proposition 4 is a quick reduction from $(\mathbb{A}^+)^n \setminus \{0^n\}$ to $(\mathbb{A}^{++})^n$.

LEMMA 6. *Given an $\mathbb{A}$-submodule $\mathcal{M}$ of $\mathbb{A}^n$ and a non-empty subset $I \subset \{1, \ldots, n\}$, define the following $\mathbb{A}$-submodule of $\mathbb{A}^I$:*

$$\mathcal{M}_I := \left\{ (f_i)_{i \in I} \;\middle|\; \sum_{i \in I} f_i e_i \in \mathcal{M} \right\} \subset \mathbb{A}^I.$$

Then $\mathcal{M}$ contains an element in $(\mathbb{A}^+)^n \setminus \{0^n\}$ if and only if there exists some non-empty set $I \subset \{1, \ldots, n\}$ such that $\mathcal{M}_I \cap (\mathbb{A}^{++})^I \neq \emptyset$.

PROOF. If $\mathcal{M}$ contains an element $f = \sum_{i=1}^n f_i e_i \in (\mathbb{A}^+)^n \setminus \{0^n\}$. Let I be the set $\{i \mid f_i \neq 0\}$. Then $(f_i)_{i \in I} \in \mathcal{M}_I \cap (\mathbb{A}^{++})^I \neq \emptyset$.

If there exists non-empty $I \subset \{1, \ldots, n\}$ such that $\mathcal{M}_I \cap (\mathbb{A}^{++})^I \neq \emptyset$. Let $(f_i)_{i \in I} \in \mathcal{M}_I \cap (\mathbb{A}^{++})^I$, then $\sum_{i=1}^n f_i e_i \in \mathcal{M} \cap (\mathbb{A}^+)^n \setminus \{0^n\} \neq \emptyset$. □

Given a finite basis for the $\mathbb{A}$-submodule $\mathcal{M}$ of $\mathbb{A}^n$, it is easy to compute $\mathcal{M}_I$ for any $I \subset \{1, \ldots, n\}$ using linear algebra over $\mathbb{A}$ [2]. Therefore it suffices to devise a procedure that decide whether $\mathcal{M} \cap (\mathbb{A}^{++})^n \neq \emptyset$ for a given $\mathcal{M}$. This procedure can then be used to decide whether $\mathcal{M} \cap (\mathbb{A}^+)^n \setminus \{0^n\} \neq \emptyset$ by verifying whether there exists non-empty $I \subset \{1, \ldots, n\}$ such that $\mathcal{M}_I \cap (\mathbb{A}^{++})^I \neq \emptyset$.

LEMMA 7. *Let $\mathcal{M} = g_1 \mathbb{A} + \cdots + g_m \mathbb{A}$ be an $\mathbb{A}$-submodule of $\mathbb{A}^n$. Define $\mathcal{M}_\mathbb{B} := g_1 \mathbb{B} + \cdots + g_m \mathbb{B}$; it is a $\mathbb{B}$-submodule of $\mathbb{B}^n$. Then $\mathcal{M} \cap (\mathbb{A}^{++})^n \neq \emptyset$ if and only if $\mathcal{M}_\mathbb{B} \cap (\mathbb{B}^{++})^n \neq \emptyset$.*

PROOF. Obviously $\mathcal{M} \subset \mathcal{M}_\mathbb{B}$ and $\mathbb{A}^{++} \subset \mathbb{B}^{++}$, so $\mathcal{M} \cap (\mathbb{A}^{++})^n \neq \emptyset \implies \mathcal{M}_\mathbb{B} \cap (\mathbb{B}^{++})^n \neq \emptyset$.

For the other direction, suppose $\mathcal{M}_\mathbb{B} \cap (\mathbb{B}^{++})^n \neq \emptyset$. Let $f = \sum_{i=1}^m h_i g_i \in (\mathbb{B}^{++})^n$. Then there exists $n_1, \ldots, n_k \in \mathbb{N}$ such that $X_1^{n_1} \cdots X_k^{n_k} h_i \in \mathbb{A}$ for all $1 \leq i \leq m$. So

$$X_1^{n_1} \cdots X_k^{n_k} f = \sum_{i=1}^m X_1^{n_1} \cdots X_k^{n_k} h_i g_i \in \mathcal{M} \cap (\mathbb{A}^{++})^n.$$

□

By Lemma 7, it suffices to consider finitely generated $\mathbb{B}$-submodules of $\mathbb{B}^n$. The key ingredient of our proof is the following consequence of a deep result by Einsiedler, Mouat, and Tuncel [7].

LEMMA 8 (COROLLARY OF [7, PROCEDURE 6.3]). *Suppose a finite basis of a submodule $\mathcal{M}_\mathbb{B}$ of $\mathbb{B}^n$ is given. One can decide whether $\mathcal{M}_\mathbb{B} \cap (\mathbb{B}^{++})^n \neq \emptyset$, provided an effective procedure for the following problem:*

- *(**ExistPos**): Given a rectangular set $K := [p, q]^d \subset \mathbb{R}_{>0}^d$, decide if for all $a \in K$ there exists $f = (f_1, \ldots, f_n) \in \mathcal{M}_\mathbb{B}$ such that $f(a) := (f_1(a), \ldots, f_n(a)) \in \mathbb{R}_{>0}^n$.*

Furthermore, we can find an element of $\mathcal{M}_\mathbb{B} \cap (\mathbb{B}^{++})^n$ with rational coefficients if the set is non-empty.

PROOF. Consider the result of Einsiedler, Mouat, and Tuncel [7, Procedure 6.3]. By the remark following Procedure 6.3, this procedure becomes effective if [7, Condition 1.3(a)] can be checked algorithmically for the compact set K defined in [7, Lemma 5.3].[2] Therefore, it suffices to provide an effective procedure that checks [7, Condition 1.3(a)] for the compact set K. By the proof of [7, Lemma 5.3], one can even suppose K to be of the form $[p, q]^d \subset \mathbb{R}_{>0}^d$. Then [7, Condition 1.3(a)] is equivalent to the problem **ExistPos**. □

LEMMA 9. *Fix an $a \in \mathbb{R}_{>0}^k$ and let $\mathcal{M}_\mathbb{B} = g_1 \mathbb{B} + \cdots + g_m \mathbb{B}$. Then the two following conditions are equivalent:*

(i) There exists $f = (f_1, \ldots, f_n) \in \mathcal{M}_\mathbb{B}$ such that $f(a) \in \mathbb{R}_{>0}^n$.
(ii) There exists reals $r_1, \ldots, r_m \in \mathbb{R}$ such that $\sum_{i=1}^m r_i g_i(a) \in \mathbb{R}_{>0}^n$.

PROOF. (i) $\implies$ (ii). Let $f \in \mathcal{M}_\mathbb{B}$ such that $f(a) \in \mathbb{R}_{>0}^n$. Suppose $f = \sum_{j=1}^m h_j g_j$ for some $h_1, \ldots, h_m \in \mathbb{B}$, then we have $f(a) = \sum_{j=1}^m h_j(a) g_j(a)$. Taking $r_1 := h_1(a), \ldots, r_m := h_m(a)$ yields (ii).

(ii) $\implies$ (i). Let $r_1, \ldots, r_m \in \mathbb{R}$ be reals such that $\sum_{i=1}^m r_i g_i(a) \in \mathbb{R}_{>0}^n$. Taking $f := \sum_{i=1}^m r_i g_i \in \mathcal{M}$ yields (i). □

PROPOSITION 10. *Suppose a finite basis of a submodule $\mathcal{M}$ of $\mathbb{A}^n$ is given. One can decide whether $\mathcal{M} \cap (\mathbb{A}^{++})^n \neq \emptyset$.*

PROOF. By Lemma 7, it suffices to decide whether $\mathcal{M}_\mathbb{B} \cap (\mathbb{B}^{++})^n \neq \emptyset$. By Lemma 8, it suffices to give a decision procedure for the problem **ExistPos**. By Lemma 9, **ExistPos** has a positive answer if and

---

[2]The second question mentioned in the remark (whether there is a computable bound on ℓ in the procedure?) does not hinder decidability since the existence of ℓ is guaranteed, according to the remark.

only if the following statement in the first order theory of reals is true:

$$\forall a_1 \cdots \forall a_d \exists r_1 \cdots \exists r_m,$$

$$\left(a_1 \in [p,q] \wedge \cdots \wedge a_d \in [p,q] \right) \implies \sum_{i=1}^{m} r_i g_i(a_1, \ldots, a_d) \in \mathbb{R}_{>0}^{n}. \tag{11}$$

The truth of such statements is decidable by Tarski's theorem [15]. □

Combining Lemma 6 and Proposition 10 immediately yields Proposition 4.

Proof of Proposition 4. By Lemma 6, $\mathcal{M}$ contains an element of $\left(\mathbb{A}^+ \right)^n \setminus \{0^n\}$ if and only if there exists a non-empty set $I \subset \{1, \ldots, n\}$ such that $\mathcal{M}_I \cap \left(\mathbb{A}^{++} \right)^I \neq \emptyset$. Therefore, it suffices to enumerate all non-empty sets $I \subset \{1, \ldots, n\}$, compute a basis for $\mathcal{M}_I$, and use Proposition 10 (with $n := \mathrm{card}(I)$) to check whether $\mathcal{M}_I \cap \left(\mathbb{A}^{++} \right)^I \neq \emptyset$. □

7 CONCLUSION AND FUTURE WORK

In this paper we proved decidability of termination of linear loops under commutative updates, where the guard condition is a polyhedral cone. A natural continuation of our work would be to generalize Theorem 5 to the case where C is a polyhedron (instead of a polyhedral cone). Unfortunately, the duality argument that is crucial in our proof stops working when we remove the homogeneity of the guard conditions. New techniques, possibly combining geometric and algebraic arguments, might be needed to overcome this difficulty. Another possible generalization is the removal of the commutativity assumption on the update matrices. For this, one would need a generalization of Einsiedler, Mouat, and Tuncel's result to left-modules over non-commutative polynomials rings, which would have deep consequences in the field of real algebra.

REFERENCES

[1] László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene M. Luks. 1996. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*. 498–507.

[2] Erwin H. Bareiss. 1968. Sylvester's identity and multistep integer-preserving Gaussian elimination. *Mathematics of computation* 22, 103 (1968), 565–578.

[3] Amir M Ben-Amram, Jesús J Doménech, and Samir Genaim. 2019. Multiphase-linear ranking functions and their relation to recurrent sets. In *International Static Analysis Symposium*. Springer, 459–480.

[4] Amir M. Ben-Amram and Samir Genaim. 2014. Ranking functions for linear-constraint loops. *Journal of the ACM (JACM)* 61, 4 (2014), 1–55.

[5] Stephen Boyd and Lieven Vandenberghe. 2004. *Convex Optimization*. Cambridge University Press.

[6] Mark Braverman. 2006. Termination of integer linear programs. In *International conference on computer aided verification*. Springer, 372–385.

[7] Manfred Einsiedler, Robert Mouat, and Selim Tuncel. 2003. When Does a Submodule of $(\mathbb{R}[x_1, \ldots, x_k])^n$ Contain a Positive Element? *Monatshefte für Mathematik* 140, 4 (2003), 267–283.

[8] Mehran Hosseini, Joël Ouaknine, and James Worrell. 2019. Termination of Linear Loops over the Integers. In *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece (LIPIcs, Vol. 132)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 118:1–118:13. https://doi.org/10.4230/LIPIcs.ICALP.2019.118

[9] Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. 2018. Polynomial invariants for affine programs. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*. 530–539.

[10] Bertrand Jeannet, Peter Schrammel, and Sriram Sankaranarayanan. 2014. Abstract acceleration of general linear loops. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. 529–540.

[11] Zachary Kincaid, Jason Breck, John Cyphert, and Thomas Reps. 2019. Closed forms for numerical loops. *Proceedings of the ACM on Programming Languages* 3, POPL (2019), 1–29.

[12] Engel Lefaucheux, Joël Ouaknine, David Purser, and James Worrell. 2021. Porous invariants. In *International Conference on Computer Aided Verification*. Springer, 172–194.

[13] Joël Ouaknine, Amaury Pouly, João Sousa-Pinto, and James Worrell. 2019. On the decidability of membership in matrix-exponential semigroups. *Journal of the ACM (JACM)* 66, 3 (2019), 1–24.

[14] Joël Ouaknine and James Worrell. 2014. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the twenty-fifth annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM, 366–379.

[15] Alfred Tarski. 1951. *A Decision Method for Elementary Algebra and Geometry*. second ed., rev., Univ. of California Press, Berkeley.

[16] Ashish Tiwari. 2004. Termination of linear programs. In *International Conference on Computer Aided Verification*. Springer, 70–82.