INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Necessary and Sufficient Condition for Termination of Linear Programs

Rachid Rebiha   *Nadir Matringe*
Arnaldo V. Moura

Technical Report - IC-13-07 - Relatório Técnico

February - 2013 - Fevereiro

The contents of this report are the sole responsibility of the authors.
O conteúdo do presente relatório é de única responsabilidade dos autores.

Necessary and Sufficient Condition for Termination of Linear Programs

Rachid Rebiha[*] Nadir Matringe [†] Arnaldo Vieira Moura[‡]

Abstract

We describe new decidability results that respond completely to major conjectures on termination analysis of linear loop programs, on all initial values interpreted over the reals. To the best of our knowledge, we present the first necessary and sufficient conditions from which we provide a complete decidability result and methods for termination analysis of such a class of programs. We reduce the termination analsysis for such programs to the problem consisting in checking if a specific vector (related to the loop condition encoding) belong to a specific vectorial space related to the matrix encoding the assignements of the loop variables. We provide theoretical results guaranteeing the soundness and completeness of the termination analysis while restrincting the variables interpretation over a specific countable subring of the field of real numbers.

1 Introduction

Formal methods for program verification research [1, 2, 3, 4] aim at discovering mathematical techniques and developing their associated algorithms to establish the correctness of software, hardware, concurrent systems, embedded systems or hybrid systems. Static program analysis [5, 2, 6], is used to check that a software is free of defects, such as buffers over flow or segmentation faults, which are safety properties, or termination and non-termination, which are liveness properties.

Proving termination of while loop programs is necessary for the verification of liveness properties, that any well behaved engineered system, safety critcal systems and embedded systems must guarantee. We could list here many verification approaches that are only practical, depending on the facility with which termination can be automatically determinated (e.g., verification of temporal properties of infinite state systems [7] is an other example.). More recent work on automated termination analysis of imperative loop programs has focused on a partial decision procedure based on the discovery and the synthesis of ranking functions. Such function maps the loop variable to a well-defined domain where their value decreases further at each iteration of the loop [8, 9]. Several interesting approaches, based

[*] Instituto de Computação, Universidade Estadual de Campinas, 13081970 Campinas, SP. Pesquisa desenvolvida com suporte financeiro da FAPESP, processo 2011089471

[†] Université de Poitiers, Laboratoire Mathématiques et Applications and Institue de Mathematiques de Jussieu Université Paris 7-Denis Diderot, France.

[‡] Instituto de Computação, Universidade Estadual de Campinas, 13081970 Campinas, SP.

on the generation of *linear* ranking functions, have been proposed [10, 11] for loop programs where the guards and the instructions can be expressed in a logic with linear arithmetic. For the generation of such functions, there are effective heuristics [12, 9], and in some cases, there are also complete methods for the synthesis of linear ranking functions [13]. On the other hand, it is easy to generate a simple linear terminant loop program that does not have a linear ranking function. And in this case the mentioned complete synthesis methods [13] fail to provide a conclusion on the termination or the non termination of such program.

In this work we address the termination problem for while linear loop programs. In other words we consider the class of loop programs where the loop condition is a conjunction of linear inequalities and the assignements to each of the variables (related to the loop instruction block), are of affine/linear form. In matrix notations, the *linear loop programs* will be represented in our most general form as:

$$\mathsf{while}\ (Bx > b),\ \{x := Ax + c\}.$$

Considering effective program transformations and simplification techniques, the termination analysis for programs presented in a more complex form can often be reduced to an analysis of a program expressed in this basic affine form. Despite tremendous progress over the years [14, 15, 16, 17, 18, 19, 20, 21], the problem of finding a practical, sound and complete method for determining termination or non termination remains very challenging for this class of programs on all initial values. We started our investigation from the line of research proposed by A.Tiwari [22].

We summarize our contributions as follows:

- First we prove a sufficient condition for the termination of homogeneous linear programs. This statement is contained in the important work proposed in [22], but the proof of the result contains a non trivially fixable mistake. The proof of this sufficient condition requires expertise in several independent mathematical fields. We show how this sufficient condition can be in used to determine termination of linear programs. We also draw its limitations.

- We then generalize the previous results. To the best of our knowledge, we present the *first necessary and sufficient condition* for the termination of linear programs. Infact, this NSC exhibits a complete decidability result for the class of linear programs on all initial values.

- Moreover, departing from this NSC, we show the scalability of our approach by demonstrating that one can directly extract a sound and complete computational method to determine termination or nontermination for linear programs.

- We provide theoretical results guaranteeing the soundness and completeness of the termination analysis while restrincting the variables interpretation over a specific countable subring of $\mathbb{R}^n$. In other words, we show that it is enough to interprete the variables over a specific countable field (or even its ring of integers) when one wants to check the termination over the reals.

The rest of this article is ordered as follows. Section 2, can be seen as a preliminary section where we introduce our computational model of programs, the notations for the rest of the paper, and the key notions of linear used in order to build our computational methods. Section 3, provides the main theoretical contributions of this work. Infact, we present our decidability results and a very useful necessary and sufficient condition allowing us to propose a complete computational method. In Section 5, we show how we interprete the variables over a countable field determining termination over the reals. Finally, Section 6 states our conclusion.

2 Linear Algebra and Linear Loop Programs

Here, we define key notions of linear algebra that are central in the theoretical and algorithmic development of our methods. If V is a *vector space* over a field $\mathbb{K}$, we write $Vect(v_1, ..., v_n)$ for the vector subspace generated by the family $v_1, ..., v_n$ of vectors of V. We denote by $\mathcal{M}(m, n, \mathbb{K})$ the set of $m \times n$ matrices with entries in $\mathbb{K}$ (and simply $\mathcal{M}(n, \mathbb{K})$ if $m = n$). If A belongs to $\mathcal{M}(m, n, \mathbb{K})$, with entry $a_{i,j}$ in position (i, j), we will sometimes denote it $(a_{i,j})$. The transpose of the matrix $A = (a_{i,j})$ is by definition the matrix $M^\top = (b_{i,j})$, such that $b_{i,j} = a_{j,i}$. The Kernel of A, also called its *nullspace*, and denoted by $Ker(A)$, is defined by: $Ker(A) = \{v \in \mathbb{K}^n \mid A \cdot v = 0_{\mathbb{K}^m}\}$. In fact, when we deal with square matrices, these Kernels are *Eigenspaces*. Let A be a $n \times n$ square matrix with entries in $\mathbb{K}$. A nonzero vector $x \in \mathbb{K}$ is an eigenvector for A associated with the eigenvalue $\lambda \in \mathbb{K}$ if: $A \cdot x = \lambda x$, i.e., $(A - \lambda I_n) \cdot x = 0$ where I_n is the $n \times n$ identity matrix. The nullspace of $(A - \lambda I_n)$ is called the *eigenspace* of A associated with eigenvalue λ. A non-zero vector x is said to be a *generalized eigenvector* for A corresponding to λ if $(A - \lambda I_n)^k \cdot x = 0$ for some positive integer k. The spaces $Ker((A - \lambda I_n)^k)$ form an increasing sequence of subspaces of k, which is stationary for $k \geq d$, for some $d \leq n$. We call the subspace $Ker((A - \lambda I_n)^d) = Ker((A - \lambda I_n)^n)$ the *generalized eigenspace* of A associated with λ.

We denote by $< , >$ the canonical scalar product on $\mathbb{R}^n$.

Notationally, as it is standard in static program analysis, a primed symbol x' refers to next state value of x after a transition is taken. First, we present *transition systems* as representations of imperative programs and *automata* as their computational models.

Definition 2.1. *A* transition system *is given by $\langle x, L, \mathcal{T}, l_0, \Theta \rangle$, where*

- *$x = (x_1, ..., x_n)$ is a set of variables,*
- *L is a set of locations and $l_0 \in L$ is the initial location.*
- *A* state *is given by an interpretation of the variables in x.*
- *A* transition *$\tau \in \mathcal{T}$ is given by a tuple $\langle l_{pre}, l_{post}, q_\tau, \rho_\tau \rangle$, where l_{pre} and l_{post} designate the pre- and post- locations of τ, and the transition relation ρ_τ is a first-order assertion over $x \cup x'$. The transition guard q_τ is a conjunction of inequalities over x, it is intuitively the pre-condition for the transition to be fired.*
- *Θ is the initial condition, given as a first-order assertion over x.*

The transition system is said to be affine *when $\rho_\mathcal{T}$ is an affine form. And it is said to be* algebraic *when $\rho_\mathcal{T}$ is an algebraic form.* □

Here, we will use the following matrix notations to represent loop programs and their associated transitions systems.

Definition 2.2. *Let P be a loop program represented by the transition system $\langle x = (x_1, ..., x_n), l_0, \mathcal{T} = \langle l_0, l_0, q_\mathcal{T}, \rho_\mathcal{T} \rangle, l_0, \Theta \rangle$. We say that P is a* linear loop program *if the following conditions hold:*

- *the loop condition (i.e. the transition guard $g_\mathcal{T}$) is a conjunction of linear inequalities. We represent the loop condition in the matrix form $Bx > b$ where $B \in \mathcal{M}(m, n, \mathbb{R})$ and $b \in \mathbb{R}^m$ (by $Bx > b$, we mean that each coordinate of the column Bx is strictly greater than the corresponding coordinate of b).*

- *the transition relation $\rho_\mathcal{T}$, representing the assignements to each of the variables, is an affine/linear form. We represent the linear assignements (related to the loop instructions block) in the matrix form $x := Ax + c$ where $A \in \mathcal{M}(n, \mathbb{R})$ and $c \in \mathbb{R}^n$.*

The linear loop program *$P = P(A, B, b, c)$ will be represented in its most general form as:* while $(Bx > b)$, $\{x := Ax + c\}$. □

In this work, we use the following linear loop program classifications.

Definition 2.3. *Let P be a linear loop program. We identify the following three type of linear loop programs, from the more specific to the more general form:*

- Homogeneous*: We denote by $P^{\mathbb{H}}$ the set of programs where all linear assignements consist of* homogeneous *expressions, and where the linear condition loop consists of at most one inequality. If P is in $P^{\mathbb{H}}$, then P will be interpreted in matrix terms as* while $(< w^\top, x >> 0)$, $\{x := Ax\}$, *where w is a $(n \times 1)$-vector corresponding to the loop condition, and where $A \in \mathcal{M}(n, \mathbb{R})$ is related to the list of assignements of the loop. We say that P has a* homogeneous *form and it will be identified as $P(A, w)$.*

- Generalized Condition*: We denote by $P^{\mathbb{G}}$ the type of linear loop programs where the condition of the loop is* generalized *to a conjonction of multiple linear inequalities. Also the considered inequalities and assignements remain as homogeneous expressions. If P is in $P^{\mathbb{G}}$ then P will be interpreted as* while $(Bx > 0)$, $\{x := Ax\}$ *where B is a $(m \times n)$-matrix corresponding to the loop condition. We say that P is in a* generalized loop condition *form and it will be identified as $P(A, B)$.*

- Affine Form*: We denote by P^{A} the set of loop programs where the inequalities and the assignements associated are generalized to affine/nonhomogeneous expressions. If P is in P^{A}, it will be interpreted as* while $(Bx > b)$, $\{x := Ax + c\}$, *for A and B as before, $b \in \mathbb{R}^m$, and $c \in \mathbb{R}^n$. We say that P is in an* affine *form and it will be identified by the signature $P(A, B, b, c)$.*

□

Example 2.1. *Consider the program depicted at the left below, for multiplying two numbers. Its computational model is described by the automaton at the right:*

(i) Pseudo code:

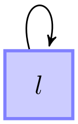
```
        ...
While (j>0){

  s := s+i;
  j := j-1;

 }
        ...
```

(ii) Transition systems:

$$\tau = \langle g_\rho = (j > 0), \rho_\tau = \begin{bmatrix} s' = s + i \\ j' = j - 1 \end{bmatrix} \rangle$$



with $V = \{s, i\}$, $\Theta = (s = 0 \wedge j = j_0)$, $l_0 = l$, $L = \{l\}$ *and* $\mathcal{T} = \{\tau\}$.

(iii) Matrix notations: $P(A, B, b, c)$ *with* $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $B = (0, 1, 0)$, $b = (0, 0, 0)^\top$ *and* $c = (0, -1, 0)^\top$. □

3 New Decibability Results for Termination of Linear Programs

In this section we introduce the theoretical foundations of our approach. Here, we provide decidability results for the termination of the complete class of linear programs.

For this section, it is enough to consider only the class of homogeneous linear programs $P^{\mathbb{H}}$ (see Definition 2.3). In fact, as we will show in section 4, the problem of termination of linear programs in $P^{\mathbb{A}}$ (i.e. the class of affine programs, see Definition 2.3) reduces to the problem of termination of homogeneous linear programs $P^{\mathbb{H}}$.

First we establish a sufficient condition for the termination of homogeneous linear programs. Then, we present the main result, which provides the first necessary and sufficient condition for the termination problem considering the complete class of linear programs. Those decidability results lead us to a complete method, associated to fast algorithms to determines termination of linear programs.

3.1 Sufficient Condition for the Termination of Homogeneous Linear Programs

Here, we prove a sufficient condition for the termination of homogeneous linear programs $P(A, w) \in P^{\mathbb{H}}$: while $(< w^\top, x >> 0)$, $\{x := Ax\}$.

Theorem 3.1. *Let* n *be a positive integer, and let* $P(A, w)$ *be program in* $P^{\mathbb{H}}$*, defined by the linear assignements encoded by a matrix* A *in* $\mathcal{M}(n, \mathbb{R})$*, and the inequality loop condition described by the vector* $w \in \mathbb{R}^n - \{0\}$*.*
If $P(A, w)$ *is nonterminant, i.e. if there exists a vector* $x \in \mathbb{R}^n$ *such that* $\langle A^k x, w\rangle > 0$ *for all* $k \geq 0$*, then* A *has a positive eigenvalue.*

This statement can actually be found as Theorem 1 of the important work proposed in [22], however, the proof of the result contains a non trivially fixable mistake, which we explain. The author of [22] applies the Brouwer's fixed point theorem to a subspace of the projective space $P(\mathbb{R}^n)$ (not $\mathbb{R}^{n-1}$ as said in [22]). However, this is not an euclidian space, and convexity is not well defined in it, hence one can't apply Brouwer's fixed point theorem to such a set. Moreover, using notations of the proof of Theorem 1 of [22], the closure NT' of the set NT can contain zero, so that its image in $P(\mathbb{R}^n)$ is not well defined. Actually this extremal case needs to be treated carefully.

Proof of Theorem 3.1

We present now the complete proof of Theorem 3.1 requires notions from in several independent mathematical fields. In fact, the core of the proof requires three lemmas and two propositions.

We first recall some basic facts about generalised eigenspaces. Let E be an $\mathbb{R}$-vector space of finite dimension, and u belong to $End_{\mathbb{R}}(E)$, the space of linear maps from E to itself. If $\lambda \in \mathbb{R}$, we denote by $E_\lambda(u)$ the subspace $\{x \in E, \exists k \geq 0, (u - I_d)^k(x) = 0\}$. This space is non zero if and only if λ is an eigenvector of u, in this case, it is called a generalised eigenspace. If χ_u is the characteristic polynomial of u, if one calls d the multiplicity of $(X - \lambda)$ in χ_u (maybe 0 if λ is not an eigenvalue), then $E_\lambda(u) = Ker(u - \lambda I_d)^d$. It is obvious that $E_\lambda(u)$ is u-stable. We denote by $Spec(u)$ the set of real eigenvalues of u.

The following property of generalised eigenspaces is well-known, and contained in the previous discussion:

Proposition 3.1. *Let E be an $\mathbb{R}$-vector space of finite dimension, and u belong to $End_{\mathbb{R}}(E)$, then $E_\lambda(u) = Ker(u-\lambda I_d)^d$, for some $d \leq n$ (in particular, $E_\lambda(u) = Ker(u-\lambda I_d)^n$, because the sequence $Ker(u - \lambda I_d)^n$ is increasing).*

Proof. We just said that one can choose d to be such that

$$(X - \lambda)^d \backslash \chi_u,$$

hence

$$d \leq d^\circ(\chi_u) = n.$$

□

We will also need the following two standard lemmas:

Lemma 3.1. *In the previous situation, there is a supplementary space E' of $E_\lambda(u)$ (i.e. $E = E_\lambda(u) \oplus E'$), and two polynomials A and B in $\mathbb{R}[X]$, such that $A(u)$ is the projection on $E_\lambda(u)$ with respect to E', and $B(u)$ is the projection on E' with respect to $E_\lambda(u)$. In particular E' is also u-stable, and for any u-stable subspace L of E, we have*

$$L = L \cap E_\lambda(u) \oplus L \cap E'.$$

Proof. Let $\chi_u = (X - \lambda)^d Q$, with $Q(\lambda) \neq 0$. By the Kernel's decomposition Lemma, we have

$$E = Ker(u - \lambda I_d)^d \oplus Ker(Q(u)).$$

We set $E' = Ker(Q(u))$. It is thus u-stable. Moreover, by Bezou's identity, there are P and P' in $\mathbb{R}[X]$, such that

$$P(u) \circ (u - \lambda I_d)^d + P'(u) \circ Q(u) = I_d,$$

then we set

$$B = P(X - \lambda)^d,$$

and

$$A = P'(u) \circ Q(u).$$

Finally, if L is u-stable, we always have

$$L \cap E_\lambda(u) \oplus L \cap E' \subset L.$$

Now write an element l of L as $l_1 + l_2$, with $l_1 \in E_\lambda(u)$, and $l_2 \in E'$, we have $A(u)(l) = l_1$, but L being u-stable, it is $A(u)$-stable as well, hence $l_1 \in L$, similarly we have $l_2 \in L$, thus

$$L = L \cap E_\lambda(u) \oplus L \cap E'.$$

□

Lemma 3.2. *Let E^* be the space $Hom_{\mathbb{R}}(E, \mathbb{R})$, for E a finite dimensional vector space, and $f_0, \ldots, f_m$ be linear forms in E^*. Then this family spans E^* if and only if $\cap_{i=0}^m Ker(f_i) = \{0\}$.*

Proof. Suppose that $f_0, \ldots, f_m$ spans E^*, then if x belongs to $\cap_{i=0}^m Ker(f_i)$, then x belongs to the kernel of any element of E^*. But then, if $B = (e_1, \ldots, e_n)$ is a basis of E, and $B^* = (e_1^*, \ldots, e_n^*)$ is its dual basis, we have $x = x_1.e_1 + \cdots + x_n.e_n$, and $e_i^*(x) = x_i = 0$, hence $x = 0$.
Conversely, if $\cap_{i=0}^m Ker(f_i) = \{0\}$, Let $g_1, \ldots, g_r$ be a maximal linearly independantfamily in $f_0, \ldots, f_m$, hence

$$Vect(g_1, \ldots, g_r) = Vect(f_0, \ldots, f_m).$$

We thus have $r \leq n$ (because $dim(E^*) = dim(E) = n$), and $\cap_{i=1}^r Ker(g_i) = \{0\}$. If r was $< n$, then $\cap_{i=1}^r Ker(g_i)$ would be an intersection of r subspaces of codimension 1, hence it would be of codimension at most r, i.e. $\cap_{i=1}^r Ker(g_i)$ would be dimension at least $n - r > 0$, which is absurd, thus $r = n$, and $(g_1, \ldots, g_r)$ is a basis of E^*, thus

$$Vect(f_0, \ldots, f_m) = E^*.$$

□

We will also use the following fact about quotient vector-spaces:

Lemma 3.3. *Let E be an $\mathbb{R}$-vector space, and u belong to $End_{\mathbb{R}}(E)$, and suppose that L is a u-stable subspace of L. Let $\overline{u} : E/L \to E/L$, be the element of $End_{\mathbb{R}}(E/L)$, defined by $u(x+L) = u(x) + L$, then $Spec(\overline{u}) \subset Spec(u)$. More generally, for any $\lambda \in Spec(\overline{u})$, the generalised eigenspace $E_\lambda(u)$ maps surjectively to $E_\lambda(\overline{u})$ in E/L.*

Proof. Let B_1 be a basis of L, and B_2 be a basis of any supplementary space. Call $\overline{B_2}$ the image of the elements of B_2 in $\overline{E} = E/L$, then $\overline{B_2}$ is a basis of $\overline{E}$. Let $B = B_1 \cup B_2$, it is a basis of B, and $Mat_B(u)$ is of the form

$$\begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}.$$

Then $X = Mat_{B_1}(u_{|L})$, and $Z = Mat_{\overline{B_2}}(\overline{u})$, and the second statement follows from this second fact.
Now if $\overline{x}$ belongs to $E_\lambda(\overline{u})$, then

$$(\overline{u} - \lambda \overline{I_d})^a \overline{x} = \overline{0}$$

for some $a \geq 0$. This means that

$$(u - \lambda I_d)^a x \in L.$$

We write $x = x_\lambda + x' \in E_\lambda(u) \oplus > E'$, for E' as in the Lemma 3.1. Then

$$(u - \lambda I_d)^a x = (u - \lambda I_d)^a x_\lambda + (u - \lambda I_d)^a x',$$

and

$$(u - \lambda I_d)^a x_\lambda \in E_\lambda(u),$$

and

$$(u - \lambda I_d)^a x' \in E'.$$

Let d be λ's multiplicity as a root of χ_u, for k large enough kd such that $kd \geq a$, we have

$$(u - \lambda I_d)^{kd} x_\lambda = 0$$

and

$$(u - \lambda I_d)^{kd} x = (u - \lambda I_d)^{kd} x'.$$

But take $P \in \mathbb{R}[X]$ as in the proof Lemma 3.1, we obtain that

$$P(u) \circ (u - \lambda I_d)^d$$

is the identity when restricted to E', in particular, this implies that

$$x' = P(u)^k (u - \lambda I_d)^{kd} x,$$

and thus $x' \in L$. Finally, we obtain

$$\overline{x} = \overline{x_\lambda},$$

and this ends the proof as $x_\lambda \in E_\lambda(u)$. □

We denote by $< \, , \, >$ the canonical scalar product on $\mathbb{R}^n$. We say that a subset of $\mathbb{R}^n$ is a convex cone if it is convex, and stable under multiplication by elements of $\mathbb{R}_{>0}$. It is obvious that an intersection of convex cones is still a convex cone, hence one can speak of the convex cone spanned by a subset of $\mathbb{R}^n$.

Proposition 3.2. *Let C be a convex cone of $\mathbb{R}^n$ non reduced to zero, and contained in the closed cone*

$$\Delta = \{x \in \ \mathbb{R}^n, \forall \ i, x_i \geq 0\}.$$

If A is an invertible endomorphism of $\mathbb{R}^n$, with $A(C) \subset C$, then A has a positive eigenvalue.

Proof. Consider $C' = C - \{0\}$, then C' is also a convex cone. It is obviously still stable under multiplication by elements of $\mathbb{R}_{>0}$. Moreover, if x and y belong to C', then for $t \in [0,1]$, the vector $tx + (1-t)y$ belongs to C by convexity, but it cannot be equal to zero, because otherwise, as both x and y have non negative coefficients, this would imply that x or y is null, which is absurd.
Now let H_1 be the affine hyperplane

$$H_1 = \{x \in \mathbb{R}^n, x_1 + \ldots x_n = 1,$$

and call f the linear form on $\mathbb{R}^n$, defined by

$$f : x \mapsto x_1 + \cdots + x_n,$$

sothat

$$H = f^{-1}(1).$$

This linear form is positive on Δ, hence we can define the projection

$$p : \Delta - \{0\} \rightarrow H,$$

given by

$$x \mapsto \frac{1}{f(x)} x,$$

it is obviously continuous. We call C_1 the set $p(C')$, we claim that

$$C_1 = C' \cap H_1,$$

in particular it is convex. Indeed, $C_1 \subset H$ by definition, and $C_1 \subset C'$ because C' is stable under $\mathbb{R}_{>0}$. Conversely, the restriction of p to $C' \cap H_1$ is the identity, hence C_1 contains $C' \cap H_1 = p(C' \cap H_1)$. It is also clearly stable under the continuous map

$$s = p \circ A : \Delta - \{0\} \rightarrow H$$

(as $A(C') \subset C'$). In particular, its closure $\overline{C_1}$ is stable under s as well. It is again convex, and compact, as a closed subset of the compact set

$$\{x \in \mathbb{R}^n, \forall \ i, \ x_i \geq 0, \ x_1 + \cdots + x_n = 1\}.$$

According to Brouwer's fixed point theorem, this implies that s has a fixed x point in

$$\overline{C_1} \subset \Delta - \{0\},$$

but we then have $A(x) = f(x)x$. As $f(x) > 0$ for any x in $\Delta - \{0\}$, this proves the Lemma. □

Finally we will prove the following statement equivalent to Theorem 3.1 (i.e., we just rewrite the statement of Theorem 3.1 in terms of morphisms just because it is more handy to work with).

Theorem 3.2. *Let E be an $\mathbb{R}$-vector space of dimension n, let u be a endomorphism of E, and f a nonzero linear form on E. If there exists a vector $x \in E$, such that $f(u^k(x)) > 0$ for all $k \geq 0$, then u has a positive eigenvalue.*

Proof. We prove this by induction on n. For $n = 1$, we can identify E with $\mathbb{R}$. Then u is of the form $x \mapsto t_u.x$, for some nonzero t_u, and $\{f \geq 0\}$ is either $\mathbb{R}_{\geq 0}$, or $\mathbb{R}_{\leq 0}$. Hence, x belongs to $\mathbb{R}_{>0}$, or $\mathbb{R}_{<0}$, and $t_u^k.x$ belongs to the same half-space for every $k \geq 0$, hence $t_u > 0$.
Now if u is non invertible, then we can replace E by $Im(u)$, and x by $u(x)$, the hypothesis are still verified by u's restriction to $Im(u)$, but $Im(u)$ being a subspace of E of strictly smaller dimension, we conclude by induction hypothesis.
We are thus left with the case u invertible. Let m be the maximal non negative integer such that $(f, f \circ u, \ldots, f \circ u^m)$ is a linearly independant family of E^*. It is easy to see that $L = \cap_{k \geq 0} Ker(f \circ u^k)$ is equal to $\cap_{k=0}^m Ker(f \circ u^k)$, hence it is u-stable. The space L is a proper subspace of E, because it is contained in $Ker(f)$. Considering the quotient space $\overline{E} = E/L$, the linear map u induces

$$\overline{u} : \overline{E} \to \overline{E},$$

and f induces a linear form $\overline{f}$ on $\bar{E}$. Let $\bar{x}$ be the image of x in E, the quadruplet

$$(\overline{E}, \overline{u}, \overline{f}, \bar{x})$$

still satisfies the hypothesis of the theorem. If L is not zero, by induction, the linear map $\overline{u}$ has a positive eigenvalue $\lambda > 0$, but λ is necessarily an eigenvalue of u by Lemma 3.3, and we are done in this case.
Otherwise $E_\lambda(u) \cap L$ is zero. Let E' be as in the statement of Lemma 3.1. In particular, as L is u-stable, we have

$$L = L \cap E_\lambda(u) \oplus L \cap E' = L \cap E',$$

hence $L \subset E'$. Now let y be a preimage of $\overline{y}$ in E, and write $y = v_0 + e'$, with $v_0 \in E_\lambda(u)$, and e' in E'. We have $u(y) = \lambda y + l$, for some l in L, as $\overline{u}(\overline{y}) = \overline{y}$. Then $u(v_0) - \lambda v_0 = -u(e') + \lambda e' + l$, but the RHS of this equality belongs to E', and the LHS to $E_\lambda(u)$, as the intersection of those spaces is zero, we deduce $u(v_0) = \lambda v_0$, and $u(e') = \lambda e' + l$. Hence in E'/L, we have

$$\lambda \in Spec(\overline{u_{|E'}}) \subset Spec(u_{|E'}),$$

```
/*...*/
 while(3x - y > 0){
   x := 3x - 2y;
   y := 4x - y;
   }
/*...*/
```

(a)

```
/*...*/
 while(z > 0){
   x:= x + y;
   z:= -z;
   }
/*...*/
```

(b)

Figure 1: Examples of homogeneous linear programs

which is absurd. This implies that

$$\overline{v_0} = \overline{y},$$

and thus v_0 is nonzero, moreover

$$f(v_0) = \overline{f}(\overline{v_0}) = \overline{f}(\overline{y}) = f(y) \geq 0,$$

and this concludes the proof when $L \neq \{0\}$.
Finally, if $L = \{0\}$, then

$$(e_1^* = f, e_2^* = f \circ u, \ldots, e_n^* = f \circ u^m)$$

is a basis of E^* according to Lemma 3.2. Take $(e_1, \ldots, e_n)$ its dual basis in E, and identify E with $\mathbb{R}^n$ thanks to this basis. Then $u^k(x)$ belongs to the space $\{v, \forall i, v_i > 0\} \subset \Delta$ for all $k \geq 0$, hence the convex cone C spanned by this family as well. It is clearly u-stable, and it is not reduced to zero as it contains x. We conclude by applying Proposition 3.2. □

Theorem 3.1 provides a sufficient condition for the termination of linear program. In other words, Theorem 3.1 says that the linear program terminates when there is no positive eigenvalues, but one can not conclude on the termination problem using theorem 3.1 if there exists at least one positive eigenvalue. Intuitively, we could say that theorem 3.1 provides us with a decidability result for the termination problem considering the subclass of linear program where the associated assignement matrix A has no positive eigenvalues (i.e., all eigenvalues are complex or negative). In the following example, we illustrate when Theorem 3.1 applies and when it does not.

Example 3.1. *Consider the homogeneous linear program 1a depicted in the figure 1 that we denote by $P(A, v)$. The associated matrix A is given by $A = \begin{pmatrix} 3 & -2 \\ 4 & -1 \end{pmatrix}$, and the vector v enconding the loop condition, is such that $v = (3, -1)^\top$. The eigenvalues of the matrix A are the complex numbers: $1 + 2i$ and $1 - 2i$. As S does not have any positive eigenvalues, we can consider the contrapose of Theorem 3.1's statement, and conclude that the program $P(A, v)$ terminates on all possible inputs.*

Example 3.2. *Now, consider the homogeneous linear program 1b depicted in Figure 1, that we denote by $P(A_1, v_1)$. The associated matrix A_1 given by $A_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, has eigenvalues 1 and -1. As A has a positive eigenvalues, one can not determine the termination (or the nontermination) of $P(A_1, v_1)$ using the theorem 3.1.*

However, We will see how to handle this case in a very automated efficient way in our more applied approach associated technicalk report [23]. □

In the next section, we generalize Theorem 3.1, and obtain stronger decidability results.

3.2 Necessary and Sufficient Condition for the Termination of Linear Program

In this section, we strengthen the theorem 3.1, in order to obtain a complete decidability result leading us to a sound and complete methods with very few computational steps executed by fast algorithms.

Infact, in the following main theorem 3.3 we provide a necessary and sufficient condition for the termination of programs $P(A, v) \in P^{\mathbb{H}}$: while $(< v^{\top}, x >> 0)$, $\{x := Ax\}$.

Theorem 3.3. *Let $A \in \mathcal{M}_n(\mathbb{R})$ and $w \neq 0 \in \mathbb{R}^n$. The program $P(A, v) : \{x := Ax, < v, x >> 0\}$ terminates if and only if for every positive eigenvalue λ of A, the generalised eigenspace $E_\lambda(A)$ is orthogonal to v (i.e. $< E_\lambda(A), v >= 0$).*

Proof of Theorem 3.3

First we will prove the following theorem written in linear algebraic terms.

Theorem 3.4. *Let E be an $\mathbb{R}$-vector space of finite dimension, let u be an endomorphism of E, and f be a nonzero linear form on E. There exists a vector $x \in E$, such that $f(u^k(x)) > 0$ for all $k \geq 0$, if and only if there is $\lambda > 0 \in Spec(u)$, such that $E_\lambda(u) \not\subset Ker(f)$.*

Proof. First suppose that here is $\lambda > 0 \in Spec(u)$, with $E_\lambda(u) \not\subset Ker(f)$. Then there is $r \geq 1$, such that $Ker(u - \lambda I_d)^{r-1} \subset Ker(f)$, but $Ker(u - \lambda I_d)^r \not\subset Ker(f)$. Let thus x be an element of $Ker(u - \lambda I_d)^r - Ker(f)$ such that $f(x) > 0$ (it is always possible, because $Ker(u - \lambda I_d)^r - Ker(f)$ is stable under $y \mapsto -y$). Because $x \in Ker(u - \lambda I_d)^r$, it is clear that $u(x) - \lambda x \in Ker(u - \lambda I_d)^{r-1}$. Then let L be $Ker(u - \lambda I_d)^{r-1}$, and $\overline{E} = E/L$. As L is u-stable, then $\overline{u}$ is well defined, and

$$\overline{u}(\overline{x}) = \lambda \overline{x}$$

because $u(x) - \lambda x \in L$. Moreover, $L \subset Ker(f)$, hence $\overline{f}$ is well defined and

$$\overline{f}(\overline{u}^k(\overline{x})) = f(u^k(x))$$

for every $k \geq 0$. As $\overline{u}^k(\overline{x}) = \lambda^k \overline{x}$, we deduce that

$$f(u^k(x)) = \lambda^k f(x) > 0$$

for all $k \geq 0$.
Conversely, suppose that there exists a vector $x \in E$, such that $f(u^k(x)) > 0$ for all $k \geq 0$, we are going to prove by induction on n that u has an eigenvalue $\lambda > 0$, such that $E_\lambda(u)$ is not contained in $Ker(f)$.
If $n = 1$, then

$$u : t \mapsto \lambda t$$

for $\lambda \in \mathbb{R}$, and thus,

$$\lambda^k(f(x)) > 0$$

for all $k \geq 0$, which implies $\lambda > 0$, and we can take $r = 1$, and $v = x$.
If $n > 1$, according to Theorem 3.2, we know that u admits positive eigenvalue μ. If $E_\mu(u)$ is not a subset of $Ker(f)$, then we are done.
If $L = E_\mu(u) \subset Ker(f)$, then we consider

$$\overline{E} = E/L.$$

This vector space is of dimension $< n$, and

$$\overline{f}(\overline{u}^k(\overline{x})) = f(u^k(x)) > 0$$

for all $k \geq 0$. By induction hypothesis, there is

$$\lambda > 0 \in Spec(\overline{u}),$$

such that

$$E_\lambda(\overline{u}) \not\subset Ker(\overline{f}).$$

But λ belongs to $Spec(u)$ according to Lemma 3.3, and $E_\lambda(u)$ maps surjectively on $E_\lambda(\overline{u})$ according to this same Lemma. In particular, we have

$$\overline{f}(E_\lambda(\overline{u})) = f(E_\lambda(u)),$$

but the LHS is not reduced to zero in this equality, hence

$$f(E_\lambda(u)) \neq \{0\},$$

i.e. $E_\lambda(u) \not\subset Ker(f)$, and this terminates the proof. □

Indeed, It has the statement of Theorem 3.3 as immediate corollary. □

Theorem 3.3 gives a necessary and sufficient condition that we use as the foundation to build a complete procedure. In order to determine termination, we have to check, for each positive eigenvalues, if the vector v, encoding the loop condition, is orthogonal to the associated generalized eigenspace. In other words we want to verify if v is orthogonal to the nullspace $Ker((A - \lambda I_n)^n)$.

Example 3.3. *Consider the program 1b depicted in Figure 1 that we denoted as $P(A_1, v_1)$. The matrix A_1 is given in Example 3.1. The vector enconding the loop condition is $v_1 = e_3 = (0, 0, 1)^\top$. We recall that A_1 has eigenvalues 1 and -1. The generalised eigenspace $E_1(A_1)$ is equal to $Vect(e_1, e_2)$, where e_1 and e_2 are the first two vectors of the canonical basis of $\mathbb{R}^3$. Hence $E_1(A_1)$ is orthogonal to v_1. According to Theorem 3.3, the program $P(A, w)$ terminates.* □

Example 3.4. *Now, if we change the loop condition of the program 1b depicted in Figure 1 to become $(y > 0)$. Then, we obtain the program $P(A_1, v_2)$ with the new considered loop condition encoded by $v_2 = e_2 = (0, 1, 0)^\top$. The eigenvalues of A_1 are (still) 1 and -1 and the generalised eigenspace $E_1(A_1) = Vect(e_1, e_2)$. Hence $E_1(A)$ is not orthogonal to v_2, because it contains v_2. Theorem 3.3 tells us that the program $P(A_1, v_2)$ does not terminate in this case.* □

In both of these examples, we are able to determine the termination/nontermination using Theorem 3.3. On the other hand, the first Theorem 3.1 does not allow us to say anything about the termination of these programs (because the assignement matrix A' exhibit at least one positive eigenvalue).

The necessary and sufficent conditions (see Theorem 3.3) and its Corollaries obtained and presented in our associated technical reports [23], allow us to determine the termination of any homogeneous linear program, considering all initial values. In section 4, we will see that the termination analysis of affine linear programs in $P^{\mathbb{A}}$, reduces to the class of homogeneous linear programs. Thus the presented necessary and sufficient condition provides a decidability result and a complete computational method for determining the termination of the full class of linear/affine programs.

Remark 3.1. *As we show in [23], we avoid the computation of generalized eigenspaces in practice, and instead, use the exact algorithms and associated corollaries obtained from Theorem 3.3 and presented in [23].*

4 Termination for Linear Programs Reduce to Homogeneous Forms

In this section we show how the termination problem for the classes $P^{\mathbb{G}}$ and $P^{\mathcal{A}}$ (see Definition 2.3) can be reduced to the problem of termination of programs in the class $P^{\mathbb{H}}$. In other words, we show how Theorem 3.3 extends to the complete class of linear programs.

4.1 From Generalized Condition to Homogeneous Programs

In this section, we treat the case where the loop condition is *generalized* to a conjunction of a finite number of linear inequalities. These inequalities are encoded by a matrix B of $\mathcal{M}(m, n, \mathbb{R})$. Let

$$P(A, B) : \mathsf{while}(Bx > 0)\{x := Ax\}$$

be a program in the class $P^{\mathbb{G}}$, where B is an element of $\mathcal{M}(m, n, \mathbb{R})$, x is a vector in $\mathbb{R}^n$ and A is an element of $\mathcal{M}(n, \mathbb{R})$. We will say that Bx is positive, and write $Bx > 0$, if each coordinate of the vector $Bx \in \mathbb{R}^m$ is > 0. If B has top row row_1, then second row row_2, ..., last bottom row row_m, and $Bx = y = (y_1, \ldots, y_m)^\top$, then $y_i = row_i.x =< row_i^\top, x >$. Hence to say that $Bx > 0$, is to say that for i between 1 and m, the scalar product $< row_i^\top, x >$ is strictly positive.

Hence, if we consider the general program associated $P(A, B)$ which does $x := Ax$ as long as $Bx > 0$, it will be terminating if and only if one of the programs $P(A, row_i^\top)$ is terminating for i between 1 and m. Following this statement, we establish the following Theorem 4.1.

Theorem 4.1. *Let A be a matrix in $\mathcal{M}(n, \mathbb{R})$ and B be a matrix in $\mathcal{M}(m, n, \mathbb{R})$. And we denote by $(row_1, \cdots row_m)$ the m row vectors of B. The program $P(A, B)$ is terminating if and only if there is $i \in 1, \ldots, m$ such that for all positive eigenvalues λ of A, the generalised eigenspace $E_\lambda(A)$ is orthogonal to $row_i^\top$.* □

Proof. if we consider the general program associated $P(A, B)$ which does $x := Ax$ as long as $Bx > 0$, it will be terminating if and only if one of the programs $P(A, row_i^\top)$ is terminating for i between 1 and m. By Theorem 3.3, we know that the statement "$P(A, row_i^\top)$ is terminating" is equivalent to say that for every positive eigenvalue λ of A, the generalised eigenspace $E_\lambda(A)$ is orthogonal to $row_i^\top$. □

The following example illustrates the application of Theorem 4.1 on two programs.

Example 4.1. *Consider the program $P(A_1, B_1)$ depicted as follow:*

(i) Pseudo code:

```
while((x+z>0)&&(x+y>0)){
   x  := 2x  +  y  +3z;
   y  := -y;
   z  := 2z;}
```

(ii) Associated matrix:

$$A_1 = \begin{pmatrix} 2 & 1 & 3 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \textit{ and } B_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Then the program $P(A_1, B_1)$ is nonterminating, because 2 is the only positive eigenvalue of A, and the generalised eigenspace $E_2(A_1) = Vect(e_1, e_3)$ has $Vect(e_2)$ as an orthognal, which contains neither $(1, 0, 1)^\top$, nor $(1, 1, 0)^\top$. □

Example 4.2. *Consider the same program depicted in 4.1, but we change the loop condition to the following one: $(x + +y + z > 0) \wedge (y > 0)$. This modified loop condition is encoded by the matrix matrix $B_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. The assignement matrix remains unchanged and we still consider A_1.*

The program $P(A_1, B_2)$ terminates because the second row of B_2 is $e_2^\top$, and e_2 is orthogonal to $E_2(A_1)$. □

4.2 Termination Analysis for Affine Programs

We ow show that the affine case reduces to the homogeneous case. Moreover, in the following procedure, we show how one can apply directly Theorem 3.3 to establish termination of affine programs.

For $A \in \mathcal{M}(n, \mathbb{R})$, $B \in \mathcal{M}(m, n, \mathbb{R})$, $b = (b_1, \ldots, b_m)^\top$ a vector in $\mathcal{M}(1, m, \mathbb{R})$ and c a vector in $\mathcal{M}(1, n, \mathbb{R})$. We denote by $P(A, B, b, c) \in P^{\mathbb{A}}$ the program which does $x := Ax + c$ as long as $Bx > b$. Now we build the matrices $A' \in \mathcal{M}(n+1, \mathbb{R})$ and $B' \in \mathcal{M}(m+1, n+1, \mathbb{R})$ as follows:

$$A' = \left(\begin{array}{ccc|c} & & & c_1 \\ & \text{A} & & \vdots \\ & & & c_n \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \qquad B' = \left(\begin{array}{ccc|c} & & & -b_1 \\ & \text{B} & & \vdots \\ & & & -b_m \\ \hline 0 & \cdots & 0 & 1 \end{array}\right)$$

We augmented the matrix A with the vector c and the row $(0, \cdots 0, 1)$, and the matrix B with the vector $-b$ and the row $(0, \cdots 0, 1)$. Here we adapt the Proposition 2 of [22] on the reduction of affine program in order to extend our necessary and sufficient condition to the class $P^{\mathbb{A}}$. The programm $P(A, B, b, c)$ terminates if and only if the homogeneous program $P(A', B')$ (which does $x' := A'x'$ as long as $B'x' > 0$) terminates. Considering the reduction of the termination analysis to the class $P^{\mathbb{H}}$ done in the previous section. We can already note that the termination analysis of programs in $P^{\mathbb{A}}$ reduces to the same analysis for programs in $P^{\mathbb{H}}$.

Theorem 4.2. *For $A \in \mathcal{M}(n, \mathbb{R})$, $B \in \mathcal{M}(m, n, \mathbb{R})$, $b = (b_1, \ldots, b_m)^\top$ a vector in $\mathcal{M}(1, m, \mathbb{R})$ and c a vector in $\mathcal{M}(1, n, \mathbb{R})$. Let $B' \in \mathcal{M}(m+1, n+1, \mathbb{R})$ and $A' \in \mathcal{M}(n+1, \mathbb{R})$ be the matrices built as such: $B' = \begin{pmatrix} B & -b \\ 0 & 1 \end{pmatrix}$ and $A' = \begin{pmatrix} A & c \\ 0 & 1 \end{pmatrix}$. We denote by row_i the i-th row of B and by r_i the i-th row of B'. By the definition of B', we have $r_1 = (row_1, -b_1), \ldots, r_m = (row_1, -b_m)$, and $r_{m+1} = (0, \ldots, 0, 1)$.*
The program $P(A, B, b, c)$ is terminating if and only if there is $i \in 1, \ldots, m+1$ such that for all positive eigenvalues λ of A', the generalised eigenspace $E_\lambda(A')$ is orthogonal to r_i. □

Proof. The programm $P(A, B, b, c)$ terminates if and only if the homogeneous program $P(A', B')$ by construction of the matrix A' and B'. To prove this statement we can thus apply directly Theorem 4.1 for $P(A', B')$. □

The following Example 4.3, illustrate the application of Theorem 4.2 on two programs.

Example 4.3. *Consider the affine program $P(A_1, B_1, b_1, c_1) \in P^{\mathbb{A}}$ depicted as follow:*

(i) Pseudo code:

```
while((x+z>1)&&(x+y>1)){
  x  :=  x  +  y  +3z+1;
  y  :=  -y;
  z  :=  z+1;}
```

(ii) Associated matrix:

$$A_1 = \begin{pmatrix} 1 & 1 & 3 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; B_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

$b_1 = (1, 1)^\top$ *and* $c_1 = (1, 0, 1)^\top$.

We define the matrix A'_1, B'_1 such that:

$$A'_1 = \begin{pmatrix} 1 & 1 & 3 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \textit{ and } B'_1 = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then the program $P(A_1, B_1, b_1, c_1)$ is nonterminating, because 1 is the only positve eigenvalue of A'_1, and the generalised eigenspace $E_1(A'_1) = Vect(e_1, e_3, e_4)$ has $Vect(e_2)$ as an orthognal, which contains none of the transpose of the rows of B'_1. □

Example 4.4. *Consider again the program depicted in 4.3, where we change the loop condition to the following one: $(x{+}{+}y{+}z > 1) \wedge (y > 0)$. This modified loop condition is encoded by the matrix matrix $B_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ and the vector $b_2 = (1, 0)^\top$. The assignment matrix remains unchanged and we still consider A_1 and c_1. Then the matrix A'_1 introduced in the previous program at Example 4.3, remains unchanged and we have $B'_2 = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.*

The program $P(A_1, B_2, b_2, c_1)$ terminates because the second row of B_2 is $e_2^\top$, but e_2 is orthogonal to $E_1(A'_1)$, and 1 is the only positive eigenvalue of A_1. □

In practice we use corollaries and the algorithms deducted from Theorem 3.3 and introduced in our associated applied technical reports [23].

5 Interpreting the Variables Over Countable Sets is Sufficient

In this section, we show that we can restrict the interpretation of the variables to a specific countable subset of $\mathbb{R}^n$ while we prove the termination over the reals.

First, we study an example, which is already interesting in itself, and which will prove that we can not restrict the interpretation of the variable to the rational field $\mathbb{Q}$ if we want to prove the termination for all real inputs.

We start with two elements of $\mathbb{Q}(\sqrt{2}) - \mathbb{Q}$, which are conjugate under the Galois group $Gal_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$, of opposite signs, and the negative one of absolute value strictly greater than the one with positive absolute value. For instance, take

$$\lambda^- = -1 - \sqrt{2}, \text{ and } \lambda^+ = -1 + \sqrt{2}.$$

They are the roots of the polynomial $P(X) = (X - \lambda^-)(X - \lambda^+) = X^2 + 2X - 1$. Now let $A = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ be the associated compagnon matrix, so that its characteristic polynomial is P, and its eigenvalues are λ^- and λ^+. Its generalised eigenspaces are easy to compute, and we find:
$E_{\lambda^-}(A) = \mathbb{R}.\begin{pmatrix} 1 \\ \lambda^- \end{pmatrix} = \mathbb{R}.e^-$ and $E_{\lambda^+}(A) = \mathbb{R}.\begin{pmatrix} 1 \\ \lambda^+ \end{pmatrix} = \mathbb{R}.e^+$. Now let $v = (1, 0)^\top$, we have $< v, e^+ >= 1$, hence, according to Theorem 3.3, the program $P(A, v)$ associated to A and

v does not terminate. We can actually locate the points of $\mathbb{R}^2$ for which the program is not terminating.

Proposition 5.1. *Let A, v and P_1 be as above, the program P_1 does not terminate for initial condition $x \in \mathbb{R}^2$, if and only if $x \in E_{\lambda^+}(A)$ and $< x, v >> 0$, i.e. $x \in \mathbb{R}_{>0}.e^+$.* □

Proof. If $x = t.e^+$, with $t > 0$, then $A^k(x) = t{\lambda^+}^k.x$, and

$$< v, A^k(x) >= t{\lambda^+}^k > 0$$

for all $k \geq 0$, hence the program does not terminate for such x as initial condition.
Conversely, suppose that x satsifies $< v, A^k(x) >> 0$ for all $k \geq 0$. Decompose x on the basis (e^-, e^+). Then $x = s.e^- + t.e^+$, and

$$A^k(x) = s{\lambda^-}^k.e^- + t{\lambda^+}^k.e^+,$$

so that $< v, A^k(x) >= s{\lambda^-}^k + t{\lambda^+}^k$.
Suppose that s is not zero. As $|\lambda^-| > |\lambda^+|$, for k large enough, the scalar $< v, A^k(x) >$ will be of the same sign as $s{\lambda^-}^k$, which is alternatively positive and negative. This is absurd, hence $s = 0$.
Now as $< v, A^k(x) >= t{\lambda^+}^k$, this imples that $t > 0$, and we the Proposition is proved. □

Proposition 5.1 leads us to the following corollary.

Corollary 5.1. *With A and v as above, the program P_1 is terminating on $\mathbb{Q}^2$, but not on $\mathbb{R}^2$* □

Proof. We already saw that P_1 does not terminate on $\mathbb{R}^2$. Now let x be an element of $\mathbb{Q}^2$. If P_1 was not terminating with x as an initial value, this would imply that x belongs to $\mathbb{R}_{>0}.e^+$ according to Lemma 5.1. However, no element of $\mathbb{Q}^2$ belongs to $\mathbb{R}_{>0}.e^+$, because the quotient of the coordinates of e^+ is not rational. This implie sthat P_1 terminates on $\mathbb{Q}^2$. □

This proves that even if A and v are rational, one can not guarantee the termination over the reals if the interpretation of the variables are restricted to rationals. It is clear that one cannot hope to produce any valid conjecture of this type if A and v have wild coefficients (transcendental for example).

However, when A and v have algebraic coefficients, thanks to Theorem 3.3, one can find a simple remedy. It is indeed enough to replace $\mathbb{Q}$ by a finite extension of the field $\mathbb{Q}$. Such an extension K is called a **number field**, and is known to be countable, indeed, it is a $\mathbb{Q}$-vector space of finite dimension (i.e. $K = \mathbb{Q}.k_1 \oplus \cdots \oplus \mathbb{Q}.k_l$ for some $l \geq 1$, and elements k_i of K).
It is moreover known that K is the fraction field of its **ring of integers** O_K, which is a free $\mathbb{Z}$-module of finite type, (in fact $O_K = \mathbb{Z}.o_1 \oplus \cdots \oplus \mathbb{Z}.o_l$ for the same $l \geq 1$, and the elements o_i can be choosed equal to the k_i, for well chosen k_i's).
We say that a number field is **real** if it is a subfield of $\mathbb{R}$.

Theorem 5.1. *Let $A \in \mathcal{M}_n(\mathbb{R})$ and $v \neq 0 \in \mathbb{R}^n$, and suppose that their coefficients are actually in $\mathbb{Q}$ (or more generally in a* ***real*** *number field K). Then there is a well-determined* ***real*** *finite extension L of $\mathbb{Q}$ (or of K in the general case) contained in $\mathbb{R}$, such that the program $P(A, v)$ associated to A and v terminates, if and only if it terminates on the countable set L^n. We can choose L to be the extension $\mathbb{Q}(\lambda_1, \ldots, \lambda_t)$ of $\mathbb{Q}$ $(K(\lambda_1, \ldots, \lambda_t)$ in general) spanned by the positive eigenvalues $(\lambda_1, \ldots, \lambda_t)$ of A. It is actually enough to check the termination of the program on O_L^n.* □

Proof. We deal with the general case, the reader not familiar with field extensions can just replace K by $\mathbb{Q}$.
It is obvious that if the program terminates, it terminates on L^n for any subset L of $\mathbb{R}$. Now $\lambda_1, \ldots, \lambda_r$ be the positive eigenvalues of A. They ar all roots of the minimal (or characteristic) polynomial Q of A, which belongs to $K[X]$, they are thus all algevbraic on K (hence on $\mathbb{Q}$, as K/Q is finite). Let $L = K(\lambda_1, \ldots, \lambda_r) \subset \mathbb{R}$. Suppose that the program P_1 does not terminate. Then there is $i \in \{1, \ldots, r\}$, such that

$$< E_{\lambda_i}, v > \neq 0$$

according to Corollary 3.3. Let r be the integer ≥ 1 such that $Ker((A - \lambda_i I_n)^r) \not\subset v^\perp$, but $Ker((A - \lambda_i I_n)^{r-1}) \subset v^\perp$. We saw in the proof of Theorem 3.3, that for any x in $Ker((A - \lambda_i I_n)^r) - Ker((A - \lambda_i I_n)^{r-1})$, such that $< v, x > 0$, the programm does not terminate. We fix such an x. Both spaces $Ker((A - \lambda_i I_n)^r)$ and $Ker((A - \lambda_i I_n)^{r-1})$ are defined by linear equations with coefficients in L, hence there is a basis of $Ker((A - \lambda_i I_n)^r)$ with coefficients in L^n, containing a basis of $Ker((A - \lambda_i I_n)^{r-1})$ with coefficients in L^n. It is easy to see, that this fact implies that

$$L^n \cap [Ker((A - \lambda_i I_n)^r) - Ker((A - \lambda_i I_n)^{r-1})]$$

is dense in

$$Ker((A - \lambda_i I_n)^r) - Ker((A - \lambda_i I_n)^{r-1})$$

(because L contains Q which is dense in R). Hence there is a sequence x_k in $L^n \cap [Ker((A - \lambda_i I_n)^r) - Ker((A - \lambda_i I_n)^{r-1})]$ wich tends to x, in particular $< v, x_k > 0$ for k large enough. The programm does thus not terminate for x_k for k such that $< v, x_k >> 0$. This shows that P_1 does not terminate on L^n. Now, the fact that P_1 doesn't terminate on O_L is a trivial consequence of the fact that any element of L is the quotient of two elements of O_l, in particular, if P_1 doesn't terminate on $x \in L^n$, take $a > 0$ in O_L, such that $ax \in O_L^n$, then the program does not terminate on ax. □

Let's see how Theorem 5.1 work on our previous example.

Example 5.1. *For the program associated to the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$, and the vector $v = (0, 1)^\top$, the field L is equal to $L = \mathbb{Q}(\lambda^+) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a \in \mathbb{Q}, b \in \mathbb{Q}\}$. It's ring of integers is equal $O_L = \mathbb{Z}(\lambda^+) = \mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$. Theorem 5.1 asserts that, as the programm $P(A, v)$ is non terminating, it is already non terminating on*

O^2_L. Indeed, Take x^+ as an intial value, then $x^+ = \begin{pmatrix} 1 \\ -1+\sqrt{2} \end{pmatrix}$ belongs to O^2_L, and the we saw that $P(A,v)$ does not terminate on x^+. □

6 Conclusion

We present the *first necessary and sufficient condition* for the termination of linear programs. Infact, this NSC exhibits a complete decidability result for the class of linear programs on all initial values and provides us with a sound, complete and fast computational method for the termination analysis of such linear programs. In practice we use additional corollaries and the algorithms introduced in our associated applied technical reports [23], in order to avoid the computation of any eigenspaces or eigenvectors. Section 5, and especially the example of this section, shows that an important notion is the locus of initial values for which a linear program terminates. In our example, it allows us to answer that the program terminates on all rational initial values. Actually, we think that this type of methods can be vastly generalised, to tackle the termination problem of linear programs on rational initial values (see conjecture 1 of [22]). Because of the difficulty of the problem, we think that it should require some non trivial Galois theory, and leave this investigation to a near future.

References

[1] Cousot, P., Cousot, R.: Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: Conf. Record of the 4th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, Los Angeles, California, ACM Press, NY (1977) 238–252

[2] Manna, Z.: Mathematical Theory of Computation. McGrw-Hill (1974)

[3] Clarke, E.M., Grumberg, O., Peled, D. MIT Press, Cambridge, MA (2000)

[4] Queille, J.P., Sifakis, J.: Specification and verification of concurrent systems in cesar. In: Proceedings of the 5th Colloquium on International Symposium on Programming, London, UK, Springer-Verlag (1982) 337–351

[5] Cousot, P., Cousot, R.: Abstract interpretation and application to logic programs. Journal of Logic Programming **13**(2–3) (1992) 103–179

[6] Cousot, P., Halbwachs, N.: Automatic discovery of linear restraints among variables of a program. In: Conference Record of the Fifth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, Tucson, Arizona, ACM Press, New York, NY (1978) 84–97

[7] Sipma, H.B., Uribe, T.E., Manna, Z.: Deductive model checking. Form. Methods Syst. Des. **15**(1) (July 1999) 49–74

[8] Colón, M., Sipma, H.: Synthesis of linear ranking functions. In: Proceedings of the 7th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2001, London, UK, UK, Springer-Verlag (2001) 67–81

[9] Col'on, M.A., Sipma, H.B.: Practical methods for proving program termination. In: In CAV2002: Computer Aided Verification, volume 2404 of LNCS, Springer (2002) 442–454

[10] Bradley, A.R., Manna, Z., Sipma, H.B.: Linear ranking with reachability. In: In CAV, Springer (2005) 491–504

[11] Bradley, A.R., Manna, Z., Sipma, H.B.: Termination analysis of integer linear loops. In: In CONCUR, Springer-Verlag (2005) 488–502

[12] Dams, D., Gerth, R., Grumberg, O.: A heuristic for the automatic generation of ranking functions. In: Workshop on Advances in Verification. (2000) 1–8

[13] Podelski, A., Rybalchenko, A.: A complete method for the synthesis of linear ranking functions. In: VMCAI. (2004) 239–251

[14] Braverman, M.: Termination of integer linear programs. In: In Proc. CAV06, LNCS 4144, Springer (2006) 372–385

[15] Bradley, A.R., Manna, Z., Sipma, H.B.: Termination of polynomial programs. In: In VMCAI'2005: Verification, Model Checking, and Abstract Interpretation, volume 3385 of LNCS, Springer (2005) 113–129

[16] Chen, H.Y., Flur, S., Mukhopadhyay, S.: Termination proofs for linear simple loops. In: Proceedings of the 19th international conference on Static Analysis. SAS'12, Berlin, Heidelberg, Springer-Verlag (2012) 422–438

[17] Cousot, P.: Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming. In: Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05), Paris, France, LNCS 3385, Springer, Berlin (January 17–19 2005) 1–24

[18] Cousot, P., Cousot, R.: An abstract interpretation framework for termination. SIGPLAN Not. **47**(1) (January 2012) 245–258

[19] Cook, B., Podelski, A., Rybalchenko, A.: Termination proofs for systems code. SIGPLAN Not. **41**(6) (June 2006) 415–426

[20] Ben-Amram, A.M., Genaim, S., Masud, A.N.: On the termination of integer loops. In: VMCAI. (2012) 72–87

[21] Ben-Amram, A.M., Genaim, S.: On the linear ranking problem for integer linear-constraint loops. In: Proceedings of the 40th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages. POPL '13, New York, NY, USA, ACM (2013) 51–62

[22] Tiwari, A.: Termination of linear programs. In Alur, R., Peled, D., eds.: Computer Aided Verification, 16th International Conference, CAV 2004, Boston, MA, USA. Volume 3114 of Lecture Notes in Computer Science., Springer (2004) 70–82

[23] Rebiha, R., Matringe, N., Moura, A.V.: A complete approach for termination analysis of linear programs. Technical Report TR-IC-13-08, Institute of Computing, University of Campinas (January 2013)