Termination of Single-Path Polynomial Loop Programs

Yi Li

Chongqing Key Lab. of Automated Reasoning and Cognition, CIGIT, CAS, Chongqing, China

Abstract. Termination analysis of polynomial programs plays a very important role in applications of safety critical software. In this paper, we investigate the termination problem of single-path polynomial loop programs (SPLPs) over the reals. For such a loop program, we first assume that the set characterized by its loop guards is closed, bounded and connected. And then, we give some conditions and prove that under such conditions, the termination of single-path loop programs is decidable over the reals.

1 Introduction

Termination analysis of loop programs is endowed with a great importance for software correctness. The popular method for termination analysis is based on the synthesis of ranking functions. Several methods have been presented in [1,4,5,6,7,11,12,13,14,15,17,22] on the synthesis of ranking functions. Also, the complexity of the linear ranking function problem for linear loops is discussed in [2,3,4,5].

For example, In 2001, Colón and Sipma [13] synthesized linear ranking functions (LRFs for short) to prove loop termination by the theory of polyhedra. For single-path linear loops, Podelski and Rybalcheko [22] first proposed a complete and efficient method for synthesizing LRFs based on linear programming when program variables range over the reals and rationals in 2004. Their method is dependent on Farkas' lemma which provides a technique to extract hidden constraints from a system of linear inequalities. Bradley et al.[6,7] extended the work presented in [13] and showed how to synthesize lexicographic LRFs with linear supporting invariants over multi-path linear constraint loops in 2005. In [12], Chen et al. gave a technique to generate non-linear ranking functions for polynomial programs by solving semi-algebraic systems. Cook et al. [14] described an automatic method for finding sound under-approximations to weakest preconditions to termination.

In 2012, [11] characterized a method to generate proofs of universal termination for linear simple loops based on the synthesis of disjunctive ranking relations. Their method is a generalization of the method given in [22]. In [17], a method was proposed by Ganty and Genaim to partition the transition relations, which can be applied to conditional termination analysis. Bagnara et al. [1] analysed termination of single-path linear constraint loops by the existence of eventual LRFs, where the eventual LRFs are linear functions that become ranking functions after a finite unrolling of the loop. In 2013, Cook et al. [15] presented a method for proving termination by Ramsey-based termination arguments instead of lexicographic termination arguments. For lasso programs, Heizmann et al. suggested a series of techniques to synthesize termination arguments in [18,19,20].

It is well known that the termination of loop programs is undecidable, even for the class of linear programs [25]. Existence of ranking function is only a sufficient (but not necessary) condition on the termination of a program. That is, it is easy to construct programs that terminate, but have no ranking functions. In contrast to the above methods for synthesizing ranking functions, [25,9] tried to detect decidable subclasses. In [25], Tiwari proves that the termination of a class of single-path loops with linear guards and assignments is decidable, providing a decision procedure via constructive proofs. Braverman [9] generalized the work of Tiwari, and showed that termination of a simple of class linear loops over the integer is decidable. Xia et al. [26] gave the NZM (Non-Zero Minimum) condition under which the termination problem of loops with linear updates and nonlinear polynomial loop conditions is decidable over the reals. In addition, there are some other methods for determining termination problem of loop programs. For instance, in [8] Bradley et al. applied finite difference trees to prove termination of multipath loops with polynomial guards and assignments. In [21], Liu et al. analyzed the termination problems for multi-path polynomial programs with equational loop guards and established sufficient conditions for termination and nontermination.

In this paper, we focus on the termination of single-path polynomial loop programs having the following form

$$\begin{aligned} P:\ & \textbf{While}\ \ \mathbf{x} \in \Omega\ \ \textbf{do} \\ & \{\mathbf{x} := F(\mathbf{x})\} \\ & \textbf{endwhile} \end{aligned} \tag{1}$$

where Ω is a closed, bounded and connected subset in $\mathbb{R}^n$, defined by a set of polynomial equations and polynomial inequalities, and $F(\mathbf{x}) : \mathbb{R}^n \to \mathbb{R}^n$, is a polynomial mapping, i.e., $F(\mathbf{x}) = (f_1(\mathbf{x}), ..., f_n(\mathbf{x}))^T$ and $f_i(\mathbf{x})$ is a polynomial in $\mathbf{x}$, for $i = 1, ..., n$. For convenience, we say that Program P is defined by Ω and $F(\mathbf{x})$, i.e., $P \triangleq P(\Omega, F(\mathbf{x}))$. We say that Program P is non-terminating over the reals, if there exists a point $\mathbf{x}^* \in \mathbb{R}^n$ such that $F^k(\mathbf{x}^*) \in \Omega$ for any $k \geq 0$. If such $\mathbf{x}^*$ does not exist, then we say Program P is terminating over the reals.

In contrast to the existing methods mentioned above, for Program P, in this paper we give some conditions such that under such conditions the termination of P can be equivalently reduced to the computation of fixed points of $F(\mathbf{x})$. That is, if such conditions are satisfied, then P is nonterminating if and only if $F(\mathbf{x})$ has at least one fixed point in Ω. Otherwise, the termination of P remains unknown. In particular, Groebner basis technique is introduced, which sometimes can reduce a given polynomial mapping to another one with simpler structure. This helps us to further analyze the termination of P, when $F(\mathbf{x})$ has complex structure. Since the computation of fixed points of F can be equivalently reduced to semi-algebraic systems solving, in this paper, for convenience, we utilize the symbolic computation tool RegularChains [10] in Maple to solve such systems.

The rest of the paper is organized as follows. Section 2 introduces some basic notion and background information regarding ranking functions, semi-algebraic systems and Groebner basis. In Section 3, we give some proper conditions and prove that if such the conditions hold, then the termination of Program P is decidable over the reals. Moreover, some examples are given to illustrate our methods. Section 4 concludes the paper.

2 Preliminaries

In the section, some basic notion on ranking functions, semi-algebraic systems and Groebner basis will be introduced first.

2.1 Semi-Algebraic Systems

Let $\mathbb{R}$ be the field of real numbers. A semi-algebraic system is a set of equations, inequations and inequalities given by polynomials. And the coefficients of those polynomials are all real numbers. Let $\mathbf{v} = (v_1, ..., v_d)^T \in \mathbb{R}^d$, $\mathbf{x} = (x_1, ..., x_n)^T \in \mathbb{R}^n$. Next, we give the definition of semi-algebraic systems (SASs for short) .

Definition 1. ***(Semi-algebraic systems)*** *A semi-algebraic system is a conjunctive polynomial formula of the following form*

$$\begin{cases} p_1(\mathbf{v},\mathbf{x}) = 0, ..., p_r(\mathbf{v},\mathbf{x}) = 0, \\ g_1(\mathbf{v},\mathbf{x}) \geq 0, ..., g_k(\mathbf{v},\mathbf{x}) \geq 0, \\ g_{k+1}(\mathbf{v},\mathbf{x}) > 0, ..., g_t(\mathbf{v},\mathbf{x}) > 0, \\ h_1(\mathbf{v},\mathbf{x}) \neq 0, ..., h_m(\mathbf{v},\mathbf{x}) \neq 0, \end{cases} \tag{2}$$

where $r > 1$, $t \geq k \geq 0$, $m \geq 0$ and all p_i's, g_i's and h_i's are polynomials in $\mathbb{R}[\mathbf{v},\mathbf{x}] \setminus \mathbb{R}$. An semi-algebraic system is called parametric if $d \neq 0$, otherwise constant, where d is the dimension of $\mathbf{v}$.

The RegularChains library offers a set of tools for manipulating semi-algebraic systems. For instance, given a parametric SAS, RegularChains provides commands for getting necessary and sufficient conditions on the parameters under which the system has real solutions.

2.2 Ranking Functions

As a popular method for determining program termination, synthesis of ranking functions has received extensive attention in these years. We recall the definition of ranking functions, as follows.

Definition 2. ***(Ranking functions for single-path polynomial loop programs)*** *Given a single-path polynomial loop program P, we say $\rho(\mathbf{x})$ is a ranking function for P, if the following formula is true over the reals,*

$$\forall \mathbf{x}, \mathbf{x}', \big(\mathbf{x} \in \Omega \wedge \mathbf{x}' = F(\mathbf{x}) \Rightarrow \rho(\mathbf{x}) \geq 0 \wedge \rho(\mathbf{x}) - \rho(\mathbf{x}') \geq 1\big). \tag{3}$$

Note that the decrease by 1 in (3) can be replaced by any positive number δ. It is well known that the existence of ranking functions for P implies that Program P is terminating. Formula (3) holds if and only if the following two Formulae hold,

$$\forall \mathbf{x}, \mathbf{x}', \big(\mathbf{x} \in \Omega \wedge \mathbf{x}' = F(\mathbf{x}) \wedge \rho(\mathbf{x}) \geq 0\big), \tag{4}$$

$$\forall \mathbf{x}, \mathbf{x}', \big(\mathbf{x} \in \Omega \wedge \mathbf{x}' = F(\mathbf{x}) \wedge \rho(\mathbf{x}) - \rho(\mathbf{x}') \geq 1\big), \tag{5}$$

We now take an example to illustrate how to synthesize ranking functions by means of RegularChains.

Example 1. Consider the below single-path polynomial program.

$$\begin{aligned} P_1: \ & \textbf{While } \ x^2 + y^2 \leq 1 \ \textbf{ do} \\ & \{x := x + 4y + 3; y := 3y + 1\} \\ & \textbf{endwhile} \end{aligned} \tag{6}$$

First, predefine a ranking function template $\rho(x, y) = ax + by + c$. we next will utilize the tool RegularChains to find a, b and c such that $\rho(x, y)$ meets Formula (4) and (5). Invoking the following commands in RegularChains,

$with(RegularChains);$

$with(SemiAlgebraicSetTools);$

$T_1 := \&E([x, y, x', y']), (x' = x + 4y + 3)\&and(y' = 3y + 1)\&and(x^2 + y^2 <= 1)$
$\quad \&implies(ax + by \geq 0);$

$T_2 := \&E([x, y, x', y']), (x' = x + 4y + 3)\&and(y' = 3y + 1)\&and(x^2 + y^2 <= 1)$
$\quad \&implies(a(x - x') + b(y - y') \geq 1);$

we get

$$(b \neq 0 \wedge \sqrt{a^2 + b^2} \leq c) \vee (b = 0 \wedge a \leq 0 \wedge -a \leq c) \vee (b = 0 \wedge - < a \wedge a \leq c),$$

and

$$0 \leq b \wedge -b \leq a \wedge a \leq -\frac{3}{7}b.$$

Thus, taking $a = -1, b = 2, c = 5$, we obtain a linear ranking function $\rho(x, y) = -x + 2y + 5$.

2.3 Polynomial Ideal and Groebner Basis

Let $\alpha = (a_1, ..., a_n)^T$ and let $\mathbf{x}^\alpha = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. Let $f = \sum_\alpha c_\alpha \mathbf{x}^\alpha$ be a polynomial in $\mathbb{R}[\mathbf{x}]$. We call c_α the coefficient of the monomial $\mathbf{x}^\alpha$. The monomials $\mathbf{x}^\alpha$'s in f can also be ordered in terms of monomial orderings, such as lexicographic order, graded lexicographic order and graded reverse lex order. We state here the following well-known results on Polynomial ideal and Groebner basis briefly.

Definition 3. *Let $\mathbb{R}[\mathbf{x}]$ be a polynomial ring. A subset $I \subset \mathbb{R}[\mathbf{x}]$ is a polynomial ideal if it satisfies:*
(i) $0 \in I$.
(ii) If $f, g \in I$, then $f + g \in I$.
(iii) If $f \in I$ and $h \in \mathbb{R}[\mathbf{x}]$, then $h \cdot f \in I$.

Definition 4. *Let $f_1, ...f_s$ be polynomials in $\mathbb{R}[\mathbf{x}]$. Set*

$$\langle f_1, ..., f_s \rangle = \{\sum_{i=1}^{s} h_i f_i : \ h_1, ..., h_s \in \mathbb{R}[\mathbf{x}]\}.$$

Then $\langle f_1, ..., f_s \rangle$ is a polynomial ideal of $\mathbb{R}[\mathbf{x}]$. We call $\langle f_1, ..., f_s \rangle$ the ideal generated by $f_1, ..., f_s$.

Definition 5. *Let k be a field, and let $f_1, ...f_s$ be polynomials in $k[\mathbf{x}]$. Then we set*

$$\mathbf{V}(f_1, ..., f_s) = \{(a_1, ..., a_n) \in k^n : \ f_i(a_1, ..., a_n) = 0 \ for \ all \ 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, ..., f_s)$ the affine variety defined by $f_1, ..., f_s$.

Definition 6. *Let $V \subset k^n$ be an affine variety. Set*

$$\mathbf{I}(V) = \{f \in k[\mathbf{x}] : \ f(a_1, ..., a_n) = 0 \ for \ all \ (a_1, ..., a_n) \in V\}.$$

Then $\mathbf{I}(V)$ is an ideal and we call it the ideal of V.

Definition 7. *Let I be an ideal. We will denote by $\mathbf{V}(I)$ the set*

$$\mathbf{V}(I) = \{(a_1, ..., a_n) \in k^n : f(a_1, ..., a_n) = 0 \ for \ all \ f \in I\}.$$

The following proposition follows from Hilbert's Basis Theorem.

Proposition 1. *With the above notion. $\mathbf{V}(I)$ is an affine variety. In particular, if $I = \langle f_1, ..., f_s \rangle$, then $\mathbf{V}(I) = \mathbf{V}(f_1, ..., f_s)$.*

The above proposition shows that even though a nonzero ideal I always contains infinitely many different polynomials, the set $\mathbf{V}(I)$ can still be defined by a finite set of polynomial equations. In particular, if $I_1 = I_2$, then $\mathbf{V}(I_1) = \mathbf{V}(I_2)$.

Definition 8. *Fix a monomial order. A finite subset $G = \{g_1, ..., g_s\}$ of an ideal I is said to be Groebner basis if*

$$\langle LT(g_1), ..., LT(g_s)\rangle = \langle LT(I)\rangle,$$

where $LT(I)$ is the set of leading terms of elements of I, and $\langle LT(I)\rangle$ is the ideal generated by the elements of $LT(I)$.

It has been proven that every ideal I other than $\{0\}$ has a Groebner basis, and any Groebner basis $G = \{g_1, ..., g_s\}$ for I is a basis having good properties. That is, $I = \langle G\rangle$. For convenience, we call G the affine Groebner basis of I, if g_i's are all affine. The computation of Groebner Basis has been implemented in Maple. For example, let $I = \langle f_1, f_2\rangle = \langle 3xy - 1, x^2 + 5y - x\rangle$. Invoking the following command,

$$Basis([f_1, f_2], plex(x, y), output = extended),$$

we can get

$$[45y^3 - 3y + 1, 15y^2 + x - 1], [[-3xy + 3y - 1, 9y^2], [1 - x, 3y]].$$

The first list is a Groebner basis of I, i.e., $G = [45y^3 - 3y + 1, 15y^2 + x - 1]$. If let

$$M_G = \begin{pmatrix} -3xy + 3y - 1, & 9y^2 \\ 1 - x, & 3y \end{pmatrix}, \qquad H = (f_1, f_2),$$

then we have $G = M_G \cdot H$. Since $I = \langle G\rangle$, every element of I can also be expressed by elements of G. For the example, invoking the commands in Maple,

– NormalForm(f1, G, plex(x, y), 'Q1')

– NormalForm(f2, G, plex(x, y), 'Q2'),

we obtain that $Q_1 = [-1, 3y], Q_2 = [5y, -15y^2 + x]$. And let

$$M_H = \begin{pmatrix} -1, & 3y \\ 5y, & -15y^2 + x \end{pmatrix}.$$

It is easy to check that $H = M_H \cdot G$.

3 Termination Analysis for SPLPs

In the section, we will give some conditions under which Program P as defined in (1) is nonterminating if and only if $F(\mathbf{x})$ has fixed points in Ω. We first give the following lemma, which enables us to build necessary and sufficient criteria for termination of several kinds of SPLPs.

Lemma 1. *Let Ω and F be defined as in (1). Let $P \triangleq P(\Omega, F(\mathbf{x}))$. If Program P is non-terminating over the reals, then for any continuous function $T(\mathbf{x})$, we have*

$$\Theta \cap \Omega \neq \emptyset,$$

where $\Theta = \{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = T(F(\mathbf{x}))\}$.

Proof. The proof is simple. Assume that there exists a continuous function $T(\mathbf{x})$, such that $\Theta \cap \Omega = \emptyset$. There are two cases to consider.

(a) $\forall \mathbf{x} \in \Omega, T(\mathbf{x}) - T(F(\mathbf{x})) > 0$.

(b) $\forall \mathbf{x} \in \Omega, T(\mathbf{x}) - T(F(\mathbf{x})) < 0$.

Consider Case (a). Since Ω is a closed, bounded and connected set, and $T - T \circ F$ is continuous, it immediately follows that

$$\forall \mathbf{x} \in \Omega.(T(\mathbf{x}) - T(F(\mathbf{x})) \geq \delta_1 > 0 \wedge T(\mathbf{x}) \geq c_1),$$

for a certain positive number δ_1 and a certain constant c_1, by properties of continuous functions. It is not difficult to see that $\frac{1}{\delta_1}(T(\mathbf{x}) - c_1)$ is a ranking function for P, which implies that Program P is terminating. This contradicts the hypothesis that Program P is non-terminating. Similar analysis can also be applicable to Case (b). We just need to notice that if Case (b) occurs, then there must exist a certain positive number δ_2 and a certain constant c_2, such that

$$\forall \mathbf{x} \in \Omega.\big(-T(\mathbf{x}) - \big(-T(F(\mathbf{x}))\big) \geq \delta_2 > 0 \wedge -T(\mathbf{x}) \geq c_2\big).$$

Hence, $\frac{1}{\delta_2}(-T(\mathbf{x}) - c_2)$ is a ranking function for P. The proof of the lemma is completed. □

Following Lemma 1, we can get the below simple result.

Corollary 1. *Let Ω and F be defined as in (1). Give a Program $P \triangleq P(\Omega, F(\mathbf{x}))$. If there exists a continuous function $T(\mathbf{x})$, such that $\{\mathbf{x} \in \mathbb{R}^n : \; T(\mathbf{x}) = T(F(\mathbf{x}))\} \cap \Omega = \emptyset$, then Program P is terminating.*

It is not difficult to see that Corollary 1 presents a sufficient (but not necessary) criteria for Program P specified by $\Omega, F(\mathbf{x})$ to be terminating. In the following, we will establish necessary and sufficient condition under which the termination problem of Program P can be equivalently reduced to the problem of existence of fixed points of $F(\mathbf{x})$. To do this, we first introduce several useful lemmas as follows.

Lemma 2. *(separating hyperplane theorem [24]) Let C and D be two convex sets of $\mathbb{R}^n$, which do not intersect, i.e., $C \cap D = \emptyset$. Then there exist $a \neq 0$ and b such that $a^T\mathbf{x} \leq b$ for all $\mathbf{x} \in C$ and $a^T\mathbf{x} \geq b$ for all $\mathbf{x} \in D$.*

Lemma 2 tells us that if C and D are two disjoint nonempty convex subsets, then there exists the affine function $a^T\mathbf{x} - b$ that is nonpositive on C and nonnegative on D. The hyperplane $\{\mathbf{x} : \; a^T\mathbf{x} = b\}$ is called a separating hyperplane for C and D. Also, we say that the affine function $a^T\mathbf{x} - b$ strictly separates C and D as defined above, if $a^T\mathbf{x} < b$ for all $\mathbf{x} \in C$ and $a^T\mathbf{x} > b$ for all $\mathbf{x} \in D$. This is called strict separation of C and D. In general, disjoint convex sets need not be strictly separated by a hyperplane. However, the following lemma tells us that in the special case when C is a closed convex set and D is a single-point set, there indeed exists a hyperplane that strictly separates C and D.

Lemma 3. *(Strict separation of a point and a closed convex set [24]) Let C be a closed convex set and $\mathbf{x}_0 \notin C$. Then there exists a hyperplane that strictly separates $\mathbf{x}_0$ from C.*

Lemma 4. *([16]) Let $S \subseteq \mathbb{R}^n$ be a closed, bounded and connected set and let $\mathcal{H}$ be a polynomial mapping. Then, the image $\mathcal{H}(S)$ of S under the polynomial mapping $\mathcal{H}$ is still closed,bounded and connected.*

Given a polynomial mapping $F(\mathbf{x}) \in (\mathbb{R}[\mathbf{x}])^m$ and a vector $\alpha \in \mathbb{Z}^m_{\geq 0}$. Let $F(\mathbf{x})^\alpha = f_1^{a_1} f_2^{a_2} \cdots f_n^{a_n}$. Let $\mathcal{M}(\mathbf{x})$ be a vector of some monomials in $\mathbf{x}$. Let m be the number of elements in $\mathcal{M}$. Let

$$\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x})).$$

Clearly, $\mathcal{H}(\mathbf{x})$ can be regarded as a polynomial mapping from k^n to k^m, where $k \in \{\mathbb{R}, \mathbb{C}\}$. For example, set $\mathbf{x} = (x_1, x_2)$, $F(\mathbf{x}) = (5x_1^2, x_1 - x_2 + 1)^T$ and $\mathcal{M}(\mathbf{x}) = (x_1, x_1x_2)^T$. Then,

$$\mathcal{H}(\mathbf{x}) = (x_1 - 5x_1^2, x_1x_2 - 5x_1^2(x_1 - x_2 + 1))^T$$

is a polynomial mapping from k^2 to k^2. In addition, for a given set Ω, define

$$\mathcal{H}(\Omega) = \{\mathcal{H}(\mathbf{x}) : \ \mathbf{x} \in \Omega\} \subseteq \mathbb{R}^m.$$

Let $\mathcal{U}(\mathbf{x}) = (u_1(\mathbf{x}), ..., u_s(\mathbf{x}))^T$ be a polynomial mapping. For convenience, we also use the same notation $\mathcal{U}(\mathbf{x})$ to denote a set of polynomials consisting of all the elements in polynomial mapping $\mathcal{U}(\mathbf{x})$. Define

$$V_{\mathbb{R}}(\mathcal{U}(\mathbf{x})) = \{\mathbf{x} \in \mathbb{R}^n : \ \mathcal{U}(\mathbf{x}) = 0\}$$
$$V_{\mathbb{C}}(\mathcal{U}(\mathbf{x})) = \{\mathbf{x} \in \mathbb{C}^n : \ \mathcal{U}(\mathbf{x}) = 0\}$$

to be the real algebraic variety and the complex algebraic variety defined by $\mathcal{U}(\mathbf{x}) = 0$, repectively.

Theorem 1. *Let Ω and F be defined as in (1). Given a Program $P \triangleq P(\Omega, F(\mathbf{x}))$. Let $\mathcal{M}(\mathbf{x})$ be a vector consisting of m monomials in $\mathbb{R}[\mathbf{x}]$. Define $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x}))$. If the following conditions are satisfied,*
(a) $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x})$,
(b) $\mathcal{H}(\Omega)$ is a convex set,
then, Program P is non-terminating over the reals if and only if $F(\mathbf{x})$ has at least one fixed point in Ω.

Proof. If $F(\mathbf{x})$ has one fixed point in Ω, then Program P does not terminate on its fixed point. Next, we will claim that if $F(\mathbf{x})$ has no fixed points in Ω, then Program P terminates. Since $F(\mathbf{x})$ has no fixed points in Ω, we know that $V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x}) \cap \Omega = \emptyset$. It immediately follows that $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) \cap \Omega = \emptyset$, since $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x})$. Therefore, for any $\mathbf{x} \in \Omega$, $\mathcal{H}(\mathbf{x}) \neq 0$. This implies that $\mathbf{0} \notin \mathcal{H}(\Omega)$, where $\mathbf{0} \in \mathbb{R}^m$, $\Omega \subseteq \mathbb{R}^n$ and

$$\mathcal{H}(\Omega) = \{\mathcal{H}(\mathbf{x}) : \ \mathbf{x} \in \Omega\} \subseteq \mathbb{R}^m.$$

Let $\mathbf{u} = \mathcal{H}(\mathbf{x})$. Since $\mathcal{H}: \mathbb{R}^n \to \mathbb{R}^m$ is a polynomial mapping and Ω is closed, bounded and connected, by Lemma 2, we know $\mathcal{H}(\Omega)$ is a closed, bounded and connected set. Also, by the hypothesis (b), we know that $\mathcal{H}(\Omega)$ is a convex set. Thus, $\mathcal{H}(\Omega)$ is a closed convex set. By Lemma 3, we know that in the space $\mathbb{R}^m$, there must exist a hyperplane $\mathbf{a}^T \cdot \mathbf{u} = \mathbf{b}$, which can strictly separate $\mathbf{0}$ from $\mathcal{H}(\Omega)$. That is to say, for any $\mathbf{u} \in \mathcal{H}(\Omega)$, $\mathbf{a}^T \cdot \mathbf{u} \neq \mathbf{b}$. Furthermore, since $\mathbf{0} \in \mathbb{R}^m$ is strictly separated from $\mathcal{H}(\Omega) \subseteq \mathbb{R}^m$ by the hyperplane $\mathbf{a}^T \cdot \mathbf{u} = \mathbf{b}$, it follows that the hyperplane $\mathbf{a}^T \cdot \mathbf{u} = \mathbf{0}$ must be disjoint from $\mathcal{H}(\Omega)$, which passes through the origin $\mathbf{0}$ and parallels to the hyperplane $\mathbf{a}^T \cdot \mathbf{u} = \mathbf{b}$. Therefore, since the hyperplane $\mathbf{a}^T \cdot \mathbf{u} = \mathbf{0}$ is disjoint from $\mathcal{H}(\Omega)$, we get that for any $\mathbf{u} \in \mathcal{H}(\Omega)$, $\mathbf{a}^T \cdot \mathbf{u} \neq \mathbf{0}$. This immediately implies that for any $\mathbf{x} \in \Omega$, we have $\mathbf{a}^T \cdot \mathcal{H}(\mathbf{x}) \neq \mathbf{0}$, since $\mathbf{u} = \mathcal{H}(\mathbf{x})$. Thus, for any $\mathbf{x} \in \Omega$, $\mathbf{a}^T \cdot (\mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x}))) \neq \mathbf{0}$. Let $T(\mathbf{x}) = \mathbf{a}^T \cdot \mathcal{M}(\mathbf{x})$. By Corollary 1, Program P must terminate, since $\{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = T(F(\mathbf{x}))\} \cap \Omega = \emptyset$. This completes the proof of the theorem. □

Remark 1. Let $S_{\mathcal{H}} = \{\mathbf{a} : \mathbf{a}^T \mathcal{H}(\mathbf{x}) \neq 0, \ for\ all\ \mathbf{x} \in \Omega\}$. By the proof of Theorem 1, we know that if the conditions (a) and (b) in the theorem are satisfied, then F has no fixed points in Ω implies that $S_{\mathcal{H}} \neq \emptyset$.

Example 2. Consider the termination of the below program.

$$\begin{aligned} P_2: \ & \textbf{While } \ 4 \leq x \leq 5 \wedge 1 \leq y \leq 2 \ \textbf{ do} \\ & \{x := x; y := -xy + y^2 + 1\} \\ & \textbf{endwhile} \end{aligned} \tag{7}$$

Let $\Omega = \{(x, y) \in \mathbb{R}^2 : \ 4 \leq x \leq 5 \wedge 1 \leq y \leq 2\}$, $f_1(x, y) = x$ and $f_2(x, y) = y^2 - xy + 1$. Let $\mathcal{M}(\mathbf{x}) = (x, y, xy)^T$. Thus,

$$\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x})) = (x - f_1, y - f_2, xy - f_1 f_2)^T.$$

Invoking the commands in RegularChains below,

/* to define the region Ω

$c_1 := x >= 4; c_2 := x <= 5; c_3 := y >= 1; c_4 := y <= 2;$

$/*$ to describe the formula $\forall x \forall y((x, y) \in V_{\mathbb{R}}(\mathcal{H}(x, y)) \Rightarrow V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x}))$

$q_1 := \&A([x, y]), ((x - f_1 = 0)\&and(y - f_2 = 0)\&and(xy - f_1 f_2 = 0))$
$\quad \&implies((x - f_1 = 0)\&and(y - f_2 = 0));$

$/*$ to describe the formula $\forall x \forall y(V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x}) \Rightarrow (x, y) \in V_{\mathbb{R}}(\mathcal{H}(x, y)))$

$q_2 := \&A([x, y]), ((x - f_1 = 0)\&and(y - f_2 = 0))\&implies((x - f_1 = 0)$
$\quad \&and(y - f_2 = 0)\&and(xy - f_1 f_2 = 0));$

$/*$ to check if Formula q_1 is true

$QuantifierElimination(q_1, output = rootof);$

$/*$ to check if Formula q_2 is true

$QuantifierElimination(q_2, output = rootof);$

we find that the conditions (a) in Theorem 1 is satisfied. Furthermore, invoking the commands as follows,

$/*$ to describe the relation between Ω and $\mathcal{H}(\Omega)$
$p_1 := \&E([x,y]), (x - f_1 = u_1)\&and(y - f_2 = u_2)\&and(xy - f_1 f_2 = u_3)$
$\quad\quad \&and(c_1)\&and(c_2)\&and(c_3)\&and(c_4);$
$/*$ to compute $\mathcal{H}(\Omega)$ by eliminating the quantified variables x and y from p_1
$QuantifierElimination(p_1, output = rootof);$

we obtain that

$$u_1 = 0 \wedge u_3 = 0 \wedge 3 \leq u_2 \leq 7,$$

which defines $\mathcal{H}(\Omega)$. That is, $\mathcal{H}(\Omega) = \{\mathbf{u} = (u_1, u_2, u_3) \in \mathbb{R}^3 : \ u_1 = 0 \wedge u_3 = 0 \wedge 3 \leq u_2 \leq 7\}$. Clearly, $\mathcal{H}(\Omega)$ is convex. Thus, the condition (b) is satisfied. Therefore, by Theorem 1, Program P_2 is terminating, since $F(\mathbf{x})$ has no fixed points in Ω.

Corollary 2. *Let Ω and F be defined as in (1). Given a Program $P \triangleq P(\Omega, F(\mathbf{x}))$. Let $\mathcal{M}(\mathbf{x})$ be a vector consisting of some monomials in $\mathbf{x}$. Let $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x}))$. If*
(a) $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x})$,
(b) Ω is a convex set and $\mathcal{H}(\mathbf{x})$ is a convexity preserving mapping,
then, Program P is non-terminating over the reals if and only if $F(\mathbf{x})$ has at least one fixed point in Ω.

Proof. The proof is simple. We just need to notice that if condition (b) holds, then we have that $\mathcal{H}(\Omega)$ is a convex set. By Theorem 1, Program P is non-terminating if and only if $F(\mathbf{x})$ has at least one fixed point in Ω. $\square$

Corollary 3. *Let Ω and F be defined as in (1). Given a Program $P \triangleq P(\Omega, F(\mathbf{x}))$. If Ω is convex and $F(\mathbf{x})$ is an affine mapping, then, Program P is non-terminating over the reals if and only if $F(\mathbf{x})$ has at least one fixed point in Ω.*

Proof. Let $\mathcal{M}(\mathbf{x}) = (x, y)^T = \mathbf{x}$. Then $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x}))$=$\mathbf{x} - F(\mathbf{x})$. Clearly, $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x})$. Besides, since both $\mathcal{M}(\mathbf{x})$ and $F(\mathbf{x})$ are affine, $\mathcal{H}(\mathbf{x})$ is an affine mapping. Therefore, $\mathcal{H}(\Omega)$ is convex, since any affine mapping is a convexity preserving mapping and Ω is convex. By Theorem 1 or Corollary 2, Program P is non-terminating over the reals if and only if $F(\mathbf{x})$ has at least one fixed point in Ω. $\square$

Define

$$\widehat{F}(\mathbf{x}) = \begin{pmatrix} f_1(x_1) \\ f_2(x_2) \\ \vdots \\ f_i(x_i) \\ \vdots \\ f_n(x_n) \end{pmatrix}, \qquad \widehat{\Omega} = \{\mathbf{x} \in \mathbb{R}^n : \ a_i \leq x_i \leq b_i, for\ all\ i = 1, ..., n\}$$

where f_i's are all polynomials, and $\widehat{\Omega}$ is a set defined by box constraints.

Corollary 4. *With the above notion. Given a Program P specified by the above $\widehat{\Omega}$ and $\widehat{F}(\mathbf{x})$. Then Program P is non-terminating over the reals if and only if $\widehat{F}(\mathbf{x})$ has at least one fixed point in $\widehat{\Omega}$.*

Proof. Take $\mathcal{M}(\mathbf{x}) = \mathbf{x} = (x_1, ..., x_n)^T$. Then, $\mathcal{H}(\mathbf{x}) = \mathbf{x} - F(\mathbf{x})$. Clearly, $\mathbb{V}_R(\mathcal{H}(\mathbf{x})) = \mathbb{V}_R(\mathbf{x} - F(\mathbf{x}))$. Let $I_i = [a_i, b_i]$ be an interval. Since $f_i(x_i)$ is a polynomial in x_i and I_i is an interval, $f_i(I_i)$ is still an interval. Set $I_i^o = f_i(I_i)$. Then, $I_1^o \times I_2^o \times \cdots \times I_n^o$ is a hyperrectangle, which clearly defines $\mathcal{H}(\widehat{\Omega})$. That is, $\mathcal{H}(\widehat{\Omega}) = I_1^o \times I_2^o \times \cdots \times I_n^o$. It is very easy to see that $\mathcal{H}(\widehat{\Omega})$ is convex. Therefore, by Theorem 1, Program P is non-terminating over the reals if and only if $\widehat{F}(\mathbf{x})$ has at least one fixed point in $\widehat{\Omega}$. $\square$

In general, for given a closed, bounded, and connected set Ω, $\mathcal{H}(\Omega)$ is not necessarily a convex set. However, this requirement can be relaxed, when the number of program variables in Program P is 2.

Theorem 2. *Let $\mathbf{x} = (x_1, x_2)^T$. Given a Program P specified by a closed, bounded and connected set $\Omega \subseteq \mathbb{R}^2$ and a polynomial mapping $F(\mathbf{x})$. Let $\mathcal{M}(\mathbf{x}) = (\mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2})^T$, where α_1, $\alpha_2 \in \mathbb{Z}^2_{\geq 0}$. Let $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x}))$. If the following conditions are satisfied,*
(a) $\mathbb{V}_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = \mathbb{V}_{\mathbb{R}}(\mathbf{x} - F(\mathbf{x}))$,
(b) For any two points $\mathbf{x}, \mathbf{y} \in \Omega$, and any $\lambda > 0$,

$$\mathcal{H}(\mathbf{x}) \neq -\lambda \cdot \mathcal{H}(\mathbf{y}),$$

then, Program P is non-terminating if and only if $F(\mathbf{x})$ has at least one fixed point in Ω.

Proof. Let $\mathbf{u} = \mathcal{H}(\mathbf{x})$. Sufficiency is clear, as the existence of fixed points in Ω of $F(\mathbf{x})$ implies that Program P does not terminate on such a fixed point. To see necessity, suppose that $F(\mathbf{x})$ has no fixed points in Ω. Therefore, for any $\mathbf{x} \in \Omega$, $\mathbf{x} - F(\mathbf{x}) \neq 0$. That is, $\mathbb{V}_{\mathbb{R}}(\mathbf{x} - F(\mathbf{x})) \cap \Omega = \emptyset$. It directly follows that $\mathbb{V}_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) \cap \Omega = \emptyset$ by the hypothesis (a). Therefore, $\mathbf{0} \notin \mathcal{H}(\Omega)$. For any $\mathcal{H}(\mathbf{x}), \mathcal{H}(\mathbf{y})$ in $\mathcal{H}(\Omega)$, by the angle formula of two vectors, we define the angle of $\mathcal{H}(\mathbf{x}), \mathcal{H}(\mathbf{y})$ as

$$\theta = cos^{-1}(\frac{\mathcal{H}(\mathbf{x})\mathcal{H}(\mathbf{y})}{|\mathcal{H}(\mathbf{x})||\mathcal{H}(\mathbf{y})|}).$$

Clearly, $\theta \geq 0$. Let $g(\mathbf{x}, \mathbf{y}) = \frac{\mathcal{H}(\mathbf{x})\mathcal{H}(\mathbf{y})}{|\mathcal{H}(\mathbf{x})||\mathcal{H}(\mathbf{y})|}$. Since $\mathbf{0} \notin \mathcal{H}(\Omega)$, g is continuous on $\Omega \times \Omega$. And cos^{-1} is also continuous on $[-1, 1]$. Hence, the composition $cos^{-1} \circ g$ of cos^{-1} and g is continuous on $\Omega \times \Omega$. Since Ω is compact implies $\Omega \times \Omega$ is compact, continuous function $cos^{-1} \circ g$ has a maximum on $\Omega \times \Omega$, i.e., there exists θ^* such that for any $(\mathbf{x}, \mathbf{y}) \in \Omega \times \Omega$, we have $\theta \leq \theta^*$. Moreover, by the hypothesis that $\mathcal{H}(\mathbf{x}) \neq -\lambda \cdot \mathcal{H}(\mathbf{y})$ for any $\mathbf{x}, \mathbf{y} \in \Omega$ and any $\lambda > 0$, we get that the angle θ of any two vectors $\mathcal{H}(\mathbf{x}), \mathcal{H}(\mathbf{y}) \in \mathcal{H}(\Omega)$ cannot be π, i.e., $\theta \neq \pi$.

We next further show that θ^* cannot be greater than π. Suppose that $\theta^* > \pi$. Then, since $0 \leq \theta \leq \theta^*$ and $cos^{-1} \circ g$ is a continuous function on $\Omega \times \Omega$, by properties of continuous function, there must exist $(\hat{\mathbf{x}}, \hat{\mathbf{y}}) \in \Omega \times \Omega$ such that $\theta = cos^{-1}(g(\hat{\mathbf{x}}, \hat{\mathbf{y}})) = \pi$. This clearly contradicts that $\theta \neq \pi$. Therefore, we have $\theta^* < \pi$. Because $\theta^* < \pi$, there exists a closed convex sector with vertex $\mathbf{0}$, whose angle is less than π, containing the set $\mathcal{H}(\Omega)$. Since the vertex $\mathbf{0}$ of this sector is not included in $\mathcal{H}(\Omega)$, i.e., $\mathbf{0} \notin \mathcal{H}(\Omega)$, there must exist a hyperplane $\mathbf{a}^T \cdot \mathbf{u} = \mathbf{a}^T \cdot \mathcal{H}(\mathbf{x}) = \mathbf{0}$ that intersects the sector only at the origin $\mathbf{0}$. Therefore, for any $\mathcal{H}(\mathbf{x}) \in \mathcal{H}(\Omega)$, $\mathbf{a}^T \cdot \mathcal{H}(\mathbf{x}) \neq \mathbf{0}$. It immediately follows by the definition of $\mathcal{H}(\Omega)$ that for any $\mathbf{x} \in \Omega$, $\mathbf{a}^T \cdot \mathcal{H}(\mathbf{x}) \neq \mathbf{0}$. Let $T(\mathbf{x}) = \mathbf{a}^T \cdot \mathcal{M}(\mathbf{x})$. By the above arguments, we get that $\{\mathbf{x} \in \mathbb{R}^2 : \ T(\mathbf{x}) = T(F(\mathbf{x}))\} \cap \Omega = \emptyset$. By Corollary 1, Program P is terminating over the reals. This completes the proof of the theorem. $\square$

Next, we will introduce Groebner basis to analyze the termination of Program P. And the computations involved with Groebner basis and ideal will be done over $\mathbb{C}$. Given Program $P \triangleq P(F, \Omega)$ as defined in (1). Let $\mathcal{M}(\mathbf{x}) = (\mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2}, ..., \mathbf{x}^{\alpha_s})^T$. Let $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x})) = (h_1, ..., h_s)^T$ and let $G(\mathbf{x}) = (g_1, ..., g_\nu)^T$ be a Groebner basis for $\langle \mathcal{H}(\mathbf{x}) \rangle$. By the properties of Groebner basis, we have

$$\langle G(\mathbf{x}) \rangle = \langle \mathcal{H}(\mathbf{x}) \rangle \quad \text{ and } \quad M(\mathbf{x}) \cdot G(\mathbf{x}) = \mathcal{H}(\mathbf{x}), \tag{8}$$

for a certain polynomial matrix $M(\mathbf{x}) \in (\mathbb{R}[\mathbf{x}])^{s \times \nu}$. For convenience, the notation $G(\mathbf{x})$ is also used to denote a polynomial mapping from k^n to k^ν. Define

$$S = \{v \in \mathbb{R}^\nu : \ v^T \cdot G(\mathbf{x}) \neq 0, for\ all\ \mathbf{x} \in \Omega\}. \tag{9}$$

Especially, if $G(\mathbf{x})$ is an affine Groebner basis and Ω is a bounded, closed convex polytope with finitely many vertices, i.e., $G(\mathbf{x}) = A\mathbf{x} + \mathbf{c}$, $\Omega = \{\mathbf{x} \in \mathbb{R}^n : \ B\mathbf{x} \geq \mathbf{b}\}$ and for all $\mathbf{x} \in \Omega$ there exists a positive number δ such that $|\mathbf{x}| \leq \delta$, then it can be shown that $S = \cup_{i=1}^t S_i$, where S_i is a convex polytope specified by semi-algebraic system $S_i = \{v \in \mathbb{R}^\nu : \ D_i v \geq 0 \wedge \mathbf{c}_i^T v > 0\}$, for $i = 1, ..., t$. Let $\triangleright = (\geq, >)^T$. S_i can be rewritten as

$$S_i = \{v \in \mathbb{R}^\nu : \ \widetilde{D}_i v \triangleright 0\},$$

where $\widetilde{D}_i = \begin{pmatrix} D_i \\ \mathbf{c}_i^T \end{pmatrix}$.

Theorem 3. *With the above notion. Let $\Omega \subseteq \mathbb{R}^n$ be a bounded, closed and convex polytope with finitely many vertices $\mathbf{x}_1, ..., \mathbf{x}_\mu$. Let S be defined as above. If $G(\mathbf{x})$ is a affine mapping, i.e., $G(\mathbf{x}) = A\mathbf{x} + \mathbf{c}$ for some constant matrix A and some constant vector $\mathbf{c}$, then, there exist $S_1, ..., S_t$, such that $S = \cup_{i=1}^t S_i$.*

Proof. By hypothesis, since Ω is a convex set, Ω is also a connected set. Hence, since $v^T G(\mathbf{x})$ is a continuous function on the bounded, closed and connected set Ω, by the properties of continuous functions, to check if $\forall \mathbf{x} \in \Omega \Rightarrow v^T \cdot G(\mathbf{x}) \neq 0$ is equivalent to check if

(1) $\forall \mathbf{x} \in \Omega, v^T \cdot G(\mathbf{x}) > 0$, or,
(2) $\forall \mathbf{x} \in \Omega, v^T \cdot G(\mathbf{x}) < 0$.
Denote by $T_{(1)}$ and $T_{(2)}$ the sets of the vectors v's satisfying the above (1) and (2), respectively. Clearly, $S = T_{(1)} \cup T_{(2)}$. We next show that $T_{(1)} = \cup_{i=1}^{t_1} S_i$. And similar analysis can be applied to $T_{(2)}$. Consider Formula (1). Since Ω is a bounded, closed and convex polytope with finitely many vertices $\mathbf{x}_1, ..., \mathbf{x}_\mu$, every point $\mathbf{x} \in \Omega$ is a convex combination of the vertices, i.e., $\mathbf{x} = \lambda_1\mathbf{x}_1 + \lambda_2\mathbf{x}_2 + \cdots + \lambda_\mu\mathbf{x}_\mu$ where $\sum_{i=1}^{\mu} \lambda_i = 1$ and $\lambda_i \geq 0$, $i = 1, ..., \mu$. Therefore, we have

$$\forall \mathbf{x} \in \Omega \Rightarrow v^T \cdot G(\mathbf{x}) > 0$$

is equivalent to

$$\forall \bar{\lambda}.(\wedge_{i=1}^{\mu}\lambda_i \geq 0 \wedge \sum_{i=1}^{\mu} \lambda_i = 1 \Rightarrow v^T \cdot (A(\sum_{i=1}^{\mu} \lambda_i\mathbf{x}_i) + \mathbf{c}) > 0) \tag{10}$$

where $\bar{\lambda} = (\lambda_1, ..., \lambda_\mu)$ and v is regarded as parameter. Hence, eliminating the quantifiers λ_i's from (10), we get the desired $T_{(i)}$ that is a set of constraints only on v. Let $\mathbf{Obj}(\bar{\lambda}) = v^T \cdot (A(\sum_{i=1}^{\mu} \lambda_i\mathbf{x}_i) + \mathbf{c}) = \sum_{i=1}^{\mu}(v^T A\mathbf{x}_i)\lambda_i + v^T\mathbf{c}$. Clearly, Formula (10) can be converted to the following standard linear programming problem,

$$\begin{aligned} \text{minimize } & \mathbf{Obj}(\bar{\lambda}) > 0 \\ \text{subject to } & \sum_{i=1}^{\mu} \lambda_i = 1, \\ & \lambda_i \geq 0. \end{aligned} \tag{11}$$

The constraints $\{\sum_{i=1}^{\mu} \lambda_i = 1, \lambda_1 \geq 0, ..., \lambda_\mu \geq 0\}$ characterize a feasible region **Reg**. Also, it is not difficult to see that **Reg** is a simplex that has the vertices $e_1, ..., e_\mu$, where e_i denotes the vector with a 1 in the i-th coordinate and 0's elsewhere. It is well known that if the feasible region **Reg** is bounded, then the optimal solution is always one of the vertices of **Reg**. Therefore,

$$\text{minimize } \mathbf{Obj}(\bar{\lambda}) \triangleq \min(\{\mathbf{Obj}(e_i)\}_{i=1}^{\mu}),$$

where $\mathbf{Obj}(e_i) = v^T A\mathbf{x}_i + v^T\mathbf{c}$. Thus, to obtain $\mathbf{Obj}(\bar{\lambda})_{min}$ is equivalent to find the minimum value of $\{\mathbf{Obj}(e_1), ..., \mathbf{Obj}(e_\mu)\}$. Because v is regarded as parameter in (10) and (11), $\mathbf{Obj}(e_i)$'s are all linear homogenous polynomials in v with constant coefficients $(A\mathbf{x}_i + \mathbf{c})^T$. Therefore, to find the minimum value of $\{\mathbf{Obj}(e_i)\}_{i=1}^{\mu}$ and guarantee that its minimum value is positive, there will be μ cases to consider,

$$Ineq_{(1)}^{i} \triangleq \left(\bigwedge_{j \neq i} \mathbf{Obj}(e_j) \geq \mathbf{Obj}(e_i)\right) \wedge \mathbf{Obj}(e_i) > 0,$$

for $i = 1, ..., \mu$. Furthermore, since the inequalities in $Ineq^i_{(1)}$ are all linear homogenous polynomials in v, $Ineq^i_{(1)}$ can be rewritten as $Ineq^i_{(1)} \triangleq \widetilde{D}_i v \rhd 0$. And let $S_i = \{v \in \mathbb{R}^\nu : \widetilde{D}_i v \rhd 0\}$ and set $t_1 = \mu$. Then we have $T_{(1)} = \cup_{i=1}^{t_1} S_i$. Consider Formula (2). Since $\forall \mathbf{x} \in \Omega \Rightarrow v^T \cdot G(\mathbf{x}) < 0$ is equivalent to $\forall \mathbf{x} \in \Omega \Rightarrow (-v)^T \cdot G(\mathbf{x}) > 0$, we can directly construct $Ineq^i_{(2)}$ by replacing v in $Ineq^i_{(1)}$ with $-v$, i.e., $Ineq^i_{(2)} \triangleq -\widetilde{D}_i v \rhd 0$, for $i = 1, ..., \mu$. Let $S_i^- = S_{t_1+i} = \{v \in \mathbb{R}^\nu : -\widetilde{D}_i v \rhd 0\}$ for $i = 1, ..., \mu$. Then we have $T_{(2)} = \cup_{i=1}^{\mu} S_{t_1+i}$. It immediately follows that $S = T_{(1)} \cup T_{(2)} = \cup_{i=1}^{2\mu} S_i$. This completes the proof of the theorem. $\square$

Remark 2. In fact, the proof of Theorem 3 proposes a method to directly construct the desired S, if $G(\mathbf{x})$ is affine and Ω is a bounded, closed and convex polytope with finitely many vertices.

Given two matrices $A, B \in \mathbb{R}^{m \times n}$, we say $A \geq B$, if $A_{ij} \geq B_{ij}$ for all $i = 1, ..., m, j = 1, ..., n$. It is not difficult to see that if $A \geq B$, then $Av \geq Bv$ for any non-negative vector v.

Let $F(\mathbf{x}) : \mathbb{R}^n \to \mathbb{R}^n$ be a polynomial mapping. Let $\mathcal{M}(\mathbf{x}) = (\mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2}, ..., \mathbf{x}^{\alpha_s})^T$ and let $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x})) = (h_1, ..., h_s)^T$. And let $G(\mathbf{x}) = (g_1, ..., g_\nu)^T = A\mathbf{x} + \mathbf{c}$ be an affine Groebner basis for $\langle \mathcal{H}(\mathbf{x}) \rangle$. Let $S = \{v \in \mathbb{R}^\nu : v^T \cdot G(\mathbf{x}) \neq 0, for\ all\ \mathbf{x} \in \Omega\}$. By Theorem 3, we have $S = \cup_{i=1}^{t} S_i$. Let $\Omega \subseteq \mathbb{R}^n$ be a bounded, closed and convex polytope with finitely many vertices $\mathbf{x}_1, ..., \mathbf{x}_\mu$. Let $M(\mathbf{x})$ be a polynomial matrix as defined in (8). We now establish the following two results.

Theorem 4. *With the above notion. Given Program $P \triangleq P(\Omega, F)$, where F, Ω are defined as above. If there exist nonempty set $S_i = \{v \in \mathbb{R}^\nu : \widetilde{D}_i v \rhd 0\} \neq \emptyset$, $i \in \{1, ..., t\}$, and nonzero nonnegative vector $v^* \in \mathbb{R}^\nu$, such that*

$$\forall \mathbf{x} = \sum_{l=1}^{\mu} \lambda_l \mathbf{x}_l \in \Omega \Rightarrow \widetilde{D}_i M^T(\mathbf{x}) \geq \sum_{l=1}^{\mu} \lambda_l \widetilde{D}_i M^T(\mathbf{x}_l), \tag{12}$$

where $\lambda_l \geq 0$, $\sum_{l=1}^{\mu} \lambda_l = 1$ and

$$M^T(\mathbf{x}_1)v^*, M^T(\mathbf{x}_2)v^*, ..., M^T(\mathbf{x}_\mu)v^* \in S_i, \tag{13}$$

then, Program $P \triangleq P(\Omega, F)$ is terminating over the reals.

Proof. By the hypothesis, we have $S \neq \emptyset$ and

$$\forall \mathbf{x} = \sum_{l=1}^{\mu} \lambda_l \mathbf{x}_l \in \Omega \Rightarrow \widetilde{D}_i M^T(\mathbf{x}) v^* \geq \sum_{l=1}^{\mu} \lambda_l \widetilde{D}_i M^T(\mathbf{x}_l) v^*,$$

since v^* is a non-negative vector. And by (13), since for $l = 1, ..., \mu$, $M^T(\mathbf{x}_l)v^* \in S_i$, i.e., $\widetilde{D}_i M^T(\mathbf{x}_l)v^* \rhd 0$, we have $\widetilde{D}_i M^T(\mathbf{x})v^* \rhd 0$, i.e., $M^T(\mathbf{x})v^* \in S_i$. By the definition of S, we know that $(M^T(\mathbf{x})v^*)^T \cdot G(\mathbf{x}) \neq 0$ for any $\mathbf{x} \in \Omega$, since $S_i \subseteq S$.

That is, for all $\mathbf{x} \in \Omega$, $(M^T(\mathbf{x})v^*)^T \cdot G(\mathbf{x}) = (v^*)^T M(\mathbf{x}) \cdot G(\mathbf{x}) \neq 0$. Because $M(\mathbf{x})G(\mathbf{x}) = \mathcal{H}(\mathbf{x})$, we have for all $\mathbf{x} \in \Omega$,

$$(v^*)^T M(\mathbf{x}) \cdot G(\mathbf{x}) = (v^*)^T \mathcal{H}(\mathbf{x}) \neq 0.$$

Let $T(\mathbf{x}) = (v^*)^T \mathcal{M}(\mathbf{x})$. Then, we get $\{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = T(F(\mathbf{x}))\} \cap \Omega = \emptyset$. It immediately follows that Program P is terminating by Corollary 1. This completes the proof of the theorem. $\square$

Remark 3. Note that to check if Formula (12) holds is equivalent to check if

$$\forall \bar{\lambda}.(\bigwedge_{l=1}^{\mu} \lambda_l \geq 0 \wedge \sum_{l=1}^{\mu} \lambda_l = 1 \Rightarrow \widetilde{D}_i M^T(\sum_{l=1}^{\mu} \lambda_l \mathbf{x}_l) \geq \sum_{l=1}^{\mu} \lambda_l \widetilde{D}_i M^T(\mathbf{x}_l)), \tag{14}$$

since Ω is bounded convex polytope, and each point in Ω can be expressed as a convex combination of the vertices of Ω by the properties of bounded convex polytope. In addition, in terms of the definition of S_i, to check if Formula (13) holds is equivalent to check if the following semi-algebraic system,

$$v^* \geq 0 \wedge v^* \neq 0 \wedge \widetilde{D}_i M^T(\mathbf{x}_1) v^* \rhd 0 \wedge \widetilde{D}_i M^T(\mathbf{x}_2) v^* \rhd 0 \wedge \cdots \wedge \widetilde{D}_i M^T(\mathbf{x}_\mu) v^* \rhd 0. \tag{15}$$

has real solutions, where $\rhd = (\geq, >)^T$.

Theorem 5. *With the above notion. Given Program $P \triangleq P(\Omega, F)$, where F, Ω are defined as above. If the following conditions are satisfied,*
(a) $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x})$,
(b) $\mathcal{H}(\Omega) \subseteq G(\Omega)$,
then Program $P \triangleq P(\Omega, F)$ is non-terminating over the reals if and only if F has at least one fixed point in Ω.

Proof. If F has fixed points in Ω, then Program P is non-terminating. We next show that if F has no fixed points in Ω, then Program P must terminate. First, let $\mathbf{u} = G(\mathbf{x})$. And since $G(\mathbf{x})$ is an affine Groenber basis of $\langle \mathcal{H}(\mathbf{x}) \rangle$, by (8), we have $\langle \mathcal{H}(\mathbf{x}) \rangle = \langle G(\mathbf{x}) \rangle$ and $M(\mathbf{x})G(\mathbf{x}) = \mathcal{H}(\mathbf{x})$. This immediately implies that $V_{\mathbb{C}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{C}}(G(\mathbf{x}))$. Hence, $V_{\mathbb{R}}(\mathcal{H}(\mathbf{x})) = V_{\mathbb{R}}(G(\mathbf{x})) = V_{\mathbb{R}}(F(\mathbf{x}) - \mathbf{x})$, according to condition (a). Since F has no fixed points in Ω, we have $\mathbf{0} \notin G(\Omega)$, where $G(\Omega) = \{\mathbf{u} = G(\mathbf{x}) \in \mathbb{R}^\nu : \textit{ for all } \mathbf{x} \in \Omega\}$. In addition, since $G(\mathbf{x})$ is affine and Ω is a bounded, closed and convex polytope, $G(\Omega)$ is also bounded, closed and convex set. By Lemma 3 and the similar arguments presented in the proof of Theorem 1, we know that there must exist a hyperplane $v^T \cdot \mathbf{u} = \mathbf{b}$ strictly separates $\mathbf{0} \in \mathbb{R}^\nu$ from $G(\Omega) \subseteq \mathbb{R}^\nu$. That is, $v^T \cdot \mathbf{u} = \mathbf{b}$ does not intersect with $G(\Omega)$. This immediately indicates that the hyperplane $v^T \cdot \mathbf{u} = 0$ also does not intersect with $G(\Omega)$. That is, for any $\mathbf{u} \in G(\Omega)$, $v^T \cdot \mathbf{u} \neq 0$. Therefore, by the definition of $G(\Omega)$, we have for any $\mathbf{x} \in \Omega$, $v^T \cdot G(\mathbf{x}) \neq 0$. This suggests that $S = \cup_{i=1}^t S_i \neq \emptyset$. Furthermore, by condition (b), since $\mathcal{H}(\Omega) \subseteq G(\Omega)$, it immediately follows that $v^T \cdot \mathcal{H}(\Omega) \neq 0$ for any $v \in S$. This implies Program P is terminating. $\square$

Example 3. Consider the termination of the below program.

$$P_3: \ \textbf{While} \ \ 1 \le x \le 2 \wedge 1 \le y \le 2 \ \ \textbf{do}$$
$$\{x := -5x - 12; y := 3y - x^2 - 1\} \tag{16}$$
$$\textbf{endwhile}$$

Let $f_1 = -5x - 12$ and $f_2 = 3y - x^2 - 1$. Define $\Omega = \{(x, y)^T \in \mathbb{R}^2 : \ 1 \le x \le 2 \wedge 1 \le y \le 2\}$. Set VP $= \{(1, 1), (2, 1), (1, 2), (2, 2)\}$ to be a set of all vertices of Ω. And let $\mathcal{M}(\mathbf{x}) = (x, y)^T$. Then $\mathcal{H}(\mathbf{x}) = \mathcal{M}(\mathbf{x}) - \mathcal{M}(F(\mathbf{x})) = (x - f_1, y - f_2)^T$. First, invoking the command *Basis* in Maple, we get the Groebner basis of ideal $\langle \mathcal{H}(\mathbf{x}) \rangle$ and the corresponding transformation matrix $M(\mathbf{x})$,

$$G(\mathbf{x}) = (-5 + 2y, x + 2)^T,$$
$$M(\mathbf{x}) = \begin{pmatrix} 0, & 6 \\ -1, & x - 2 \end{pmatrix}.$$

Since each component in G is affine, $G(\mathbf{x})$ is an affine Groebner basis. We next check if the hypothesis in Theorem 4 holds. To do this, we first need to compute S. Let $G(\mathbf{x}) = (g_1(\mathbf{x}), g_2(\mathbf{x}))^T$ and $v = (v_1, v_2)^T$. To compute S is equivalent to eliminate quantified variables x, y from the following quantified formula:

$$\forall \mathbf{x} \in \Omega \Rightarrow v_1 \cdot g_1(\mathbf{x}) + v_2 \cdot g_1(\mathbf{x}) \ne 0. \tag{17}$$

This can be done easily, since $G(\mathbf{x})$ is affine. However, by the proof of Theorem 3 and Remark 2, we can directly construct S as follows,

$$S = \bigcup_{i=1}^{4} S_i \cup \bigcup_{i=1}^{4} S_i^- = \bigcup_{i=1}^{4} \{(v_1, v_2)^T : \ \widetilde{D}_i v \triangleright 0\} \cup \bigcup_{i=1}^{4} \{(v_1, v_2)^T : \ \widetilde{D}_i(-v) \triangleright 0\},$$

where $\triangleright = (\ge, \ge, \ge, >)^T$ and

$$\widetilde{D}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 1 & 2 \\ -1 & 7 \end{pmatrix}, \widetilde{D}_2 = \begin{pmatrix} -1 & 0 \\ -1 & 2 \\ 0 & 2 \\ 0 & 7 \end{pmatrix}, \widetilde{D}_3 = \begin{pmatrix} 0 & -2 \\ 1 & -2 \\ 1 & 0 \\ -1 & 9 \end{pmatrix}, \widetilde{D}_4 = \begin{pmatrix} -1 & -2 \\ 0 & -2 \\ -1 & 0 \\ 0 & 9 \end{pmatrix}. \tag{18}$$

Next, we will check if Formula (12) and Formula (13) hold. According to Remark 3, to check if Formula (12) and Formula (13) hold is equivalent to check if Formula (14) and Formula (15) hold. By computation, we find that when $i = 3$, both Formula (14) and Formula (15) hold. Therefore, by Theorem 4, Program P_3 must terminate over the reals.

4 Conclusion

We have analyzed the termination of single-path polynomial loop programs (SPLPs). Some conditions are given such that under such conditions the termination of this kind of loop programs over the reals can be equivalently reduced to computation of real fixed points. In other words, once such conditions are satisfied, an SPLP $P(\Omega, F)$ is not terminating over the reals if and only if F has at least one fixed point in Ω. Furthermore, such conditions can be described by quantified formulae. This enables us to apply the tools for real quantifier elimination, such as RegularChains, to automatically check if such conditions are satisfied.

Acknowledgments. The author would like to thank the anonymous reviewers for their helpful suggestions. This research is partially supported by the National Natural Science Foundation of China NNSFC(61572024, 61103110).

References

1. Bagnara, R., Mesnard, F.: Eventual linear ranking functions. Proceedings of the 15th Symposium on Principles and Practice of Declarative Programming. Madrid, Spain, ACM. pages 229-238 (2013)
2. Bagnara, R., Mesnard, F., Pescetti, A., Zaffanella, E.: A new look at the automatic synthesis of linear ranking functions. Information and Computation, 215, pages 47-67 (2012)
3. Ben-Amram, A.: The Hardness of Finding Linear Ranking Functions for Lasso Programs. Electronic Proceedings in Theoretical Computer Science, 161, pages 32-45 (2014)
4. Ben-Amram, A., Genaim, S.: On the linear ranking problem for integer linear-constraint loops. POPL '13 Proceedings of the 40th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages. Rome, Italy, ACM.pages 51-62 (2013)
5. Ben-Amram, A., Genaim, S.: Ranking Functions for Linear-Constraint Loops. Journal of the ACM 61(4), pages 1-55 (2014)
6. Bradley, A., Manna, Z., Sipma, H.: Linear Ranking with Reachability. Computer Aided Verification. K. Etessami and S. Rajamani, Springer Berlin Heidelberg. 3576: 491-504 (2005)
7. Bradley, A., Manna, Z., Sipma, H.: The Polyranking Principle. Automata, Languages and Programming. L. Caires, G. Italiano, L. Monteiro, C. Palamidessi and M. Yung, Springer Berlin Heidelberg. 3580: 1349-1361 (2005)
8. Bradley, A., Manna, Z., Sipma, H.: Termination of Polynomial Programs. Verificaton, Model Checing, and Abstract Interpretation. R. Cousot, Springer Berlin Heidelberg. 3385: 113-129 (2005)
9. Braverman, M.: Termination of Integer Linear Programs. Computer Aided Verification. T. Ball and R. Jones, Springer Berlin Heidelberg. 4144: 372-385 (2006)
10. Chen, C., Maza, M.: Quantifier Elimination by Cylindrical Algebraic Decomposition Based on Regular Chains[C]. Proceedings of the 39th International Symposium on Symbolic and Algebraic ComputationACM, pp. 91-98 (2014)
11. Chen, H., Flur, S., Mukhopadhyay, S.: Termination Proofs for Linear Simple Loops. Static Analysis. A. Miné and D. Schmidt, Springer Berlin Heidelberg. 7460: 422-438 (2012)
12. Chen, Y., Xia, B., Yang, L., Zhan, N., Zhou, C.: Discovering Non-linear Ranking Functions by Solving Semi-algebraic Systems. Theoretical Aspects of Computing-ICTAC 2007. C. Jones, Z. Liu and J. Woodcock, Springer Berlin Heidelberg. 4711: 34-49 (2007)

13. Colón, M., Sipma, H.: Synthesis of Linear Ranking Functions. Tools and Algorithms for the Construction and Analysis of Systems. T. Margaria and W. Yi, Springer Berlin Heidelberg. 2031: 67-81 (2001)
14. Cook, B., Gulwani, S., Lev-Ami, T., Rybalchenko, A., Sagiv, M.: Proving Conditional Termination. Computer Aided Verification. A. Gupta and S. Malik, Springer Berlin Heidelberg. 5123: 328-340 (2008)
15. Cook, B., See, A., Zuleger, F.: Ramsey vs. Lexicographic Termination Proving. Tools and Algorithms for the Construction and Analysis of Systems. N. Piterman and S. Smolka, Springer Berlin Heidelberg. 7795: 47-61 (2013)
16. Duistermaat, J.,Kolk, J.: Multidimensional Real Analysis. Cambridge University Press. (2004)
17. Ganty, P., Genaim, S.: Proving Termination Starting from the End. Computer Aided Verification. N. Sharygina and H. Veith, Springer Berlin Heidelberg. 8044: 397-412 (2013)
18. Heizmann, M., Hoenicke, J., Leike, J., Podelski, A.: Linear Ranking for Linear Lasso Programs. Automated Technology for Verification and Analysis. D. Van Hung and M. Ogawa, Springer International Publishing. 8172: 365-380 (2013)
19. Leike, J., Heizmann, M.: Ranking Templates for Linear Loops. Tools and Algorithms for the Construction and Analysis of Systems. E. brahm and K. Havelund, Springer Berlin Heidelberg. 8413: 172-186 (2014)
20. Leike, J., Tiwari, A.: Synthesis for Polynomial Lasso Programs. Verification, Model Checking, and Abstract Interpretation. K. McMillan and X. Rival, Springer Berlin Heidelberg. 8318: 434-452 (2014)
21. Liu, J., Xu, M., Zhan, N.J., Zhao, H.J.: Discovering non-terminating inputs for multi-path polynomial programs. J Syst Sci Complex. 27, pages 1284-1304 (2014)
22. Podelski, A., Rybalchenko, A.: A Complete Method for the Synthesis of Linear Ranking Functions. Verification, Model Checking, and Abstract Interpretation. B. Steffen and G. Levi, Springer Berlin Heidelberg. 2937: 239-251 (2004)
23. Sohn, K., Van Gelder, A.: Termination detection in logic programs using argument sizes (extended abstract), in: Proceedings of the Tenth ACM SIGACT- SIGMOD-SIGART Symposium on Principles of Database Systems, ACM, Association for Computing Machinery, Denver, CO, USA, 216C226 (1991)
24. Stephen, B., Lieven V.: Convex Optimization. Cambridge University Press. (2004)
25. Tiwari, A.: Termination of Linear Programs. Computer Aided Verification. R. Alur and D. Peled, Springer Berlin Heidelberg. 3114: 70-82 (2004)
26. Xia, B., Zhang, Z.: Termination of linear programs with nonlinear constraints. J. Symb. Comput. 45(11): 1234-1249 (2010)