Automatic Generation of Polynomial Loop Invariants: Algebraic Foundations *

Enric Rodriguez-Carbonell and Deepak Kapur

LSI Department, Technical University of Catalonia, Barcelona
erodri@lsi.upc.es
Department of Computer Science, University of New Mexico, Albuquerque
ekapur@cs.unm.edu

Abstract. In [RCK], the authors propose an abstract framework leading to a generic procedure for automating the discovery of loop invariants. This framework is then instantiated for the language of conjunctions of polynomial equations for expressing loop invariants. This paper presents the algebraic foundation of the approach. By means of algebraic geometry and polynomial ideal theory, it is proved that the procedure for finding invariants terminates if the assignment statements in the loop are solvable - in particular, affine- mappings with positive eigenvalues. This yields a correct and complete algorithm for inferring invariant conjunctions of polynomial equalities. The method has been implemented in Maple using Gröbner bases to compute intersection of ideals as well as to eliminate variables. Non-trivial invariants are generated applying this implementation to several examples to illustrate the power of the techniques.

1 Introduction

In [RCK], an abstract framework for finding invariants in loops with conditional statements and assignments is presented. It builds upon the difference equations method ([EGLW72]), which proceeds in two steps:

1. by means of recurrence equations (also called difference equations), an explicit expression is found for the value of each variable as a function of the number of loop iterations $s$, other variables that remain constant in the loop, and the input values,
2. the variable $s$ is eliminated to obtain invariant relations.

Properties of the language used for expressing invariants are identified so that a generic correct and complete procedure for computing loop invariants can be formulated. This abstract framework is then instantiated for the language of conjunctions of polynomial equalities.

* This research was partially supported by an NSF ITR award CCR-0113611, the Prince of Asturias Endowed Chair in Information Science and Technology at the University of New Mexico and an FPU grant from the Spanish Secretaría de Estado de Educación y Universidades, ref. AP2002-3093.
In this companion paper, we provide the algebraic foundation of the approach proposed in [RCK] for this language. The connection between polynomial ideal theory and loop invariants is revealed by proving that, given a loop, the polynomials \( p \) such that \( p = 0 \) is invariant, i.e., \( p \) evaluates to 0 at any program state, constitute a polynomial ideal, henceforth called the \textit{invariant ideal} of the loop. Furthermore, any conjunction of polynomial equations such that the polynomials are a basis of this ideal is inductive, in the sense that it holds when entering the loop and is preserved at each cycle; and moreover, such formula is the strongest amongst all inductive conjunctions of polynomial equalities.

One of the main results in this paper is the proof of termination of the procedure for discovering invariants in the case of loops with solvable assignments -in particular, affine- which have positive eigenvalues. In this situation, the invariant ideal is computed in at most \( 2m + 1 \) iterations, where \( m \) is the number of variables that change their value in the loop. The proof uses techniques from algebraic geometry to study the variety associated to the computed ideal at each iteration. It is shown that, at each step, either the invariant ideal has been computed, or the minimum dimension of the non-invariant irreducible components of the variety increases. Moreover, we also prove that the procedure terminates in at most \( n + 1 \) iterations if the assignment mappings commute, where \( n \) is the number of branches in the body of the loop; in particular, if there are no conditionals, the algorithm terminates in at most 2 iterations.

Besides, we show that powers of solvable mappings have “polynomial structure”. Using this fact, we explain how loop invariants can be automatically generated using Gröbner bases (see [CL98] or [AL94] as an introduction to Gröbner basis algorithm, commutative algebra and algebraic geometry, or [BW93] for a more comprehensive treatment).

The method has been implemented in Maple and has been successfully applied to several non-trivial programs, for which the inferred polynomial loop invariants have been essential when proving correctness.

The rest of the paper is organized as follows. In the next subsection, we provide brief comments about program verification, the role of loop invariants in verifying properties of imperative programs, approaches to automatically generating loop invariants and the progress made especially in recent years. After introducing the notation in Section 2, we describe the kind of loops and the domain of variables we are going to consider in Section 3. From Section 4 onwards, we focus on conjunctions of polynomial equations as loop invariants. It is shown that the set of invariant polynomials of a loop has the algebraic structure of an ideal, which immediately suggests that polynomial ideal theory and algebraic geometry can give insight into the problem of finding loop invariants. Section 5 presents the procedure for finding polynomial invariants, expressed in terms of ideals. We show in Section 6 how to implement this procedure using Gröbner bases to compute intersection of ideals and to eliminate auxiliary variables. Section 7 gives a detailed proof of termination when assignment mappings are solvable and have positive eigenvalues. We illustrate the method in Section 8 with some examples that have been studied applying our implementation in
Maple. Finally, Section 9 concludes with a summary of the contributions of the paper and an overview of future research.

1.1 Background and Related Work

In this subsection, we give some background on the importance of loop invariants in program verification and various attempts for automatically inferring them. The interested reader may look at any book on program verification for more details, as well as [RCK].

The decade of the seventies saw considerable focus on research on program verification based on Floyd-Hoare-Dijkstra’s inductive assertion method, using pre/postconditions and loop invariants. The approach has become an integral part of CS curriculum, where students are typically taught to practise such techniques by hand; however, it did not succeed in its advertised goal of mechanical verification of properties of programs. There were two main reasons for its failure:

- Theorem provers, needed to establish the validity of the verification conditions, were not well developed (both for first-order logic as well as for inductive reasoning)
- The user had to manually annotate programs with specifications and loop invariants, because the few existing tools ([GW75]) for this purpose at that moment were not powerful enough.

Nonetheless, for life-critical applications it is still imperative to verify properties of programs. With substantial progress in automated reasoning technology, several strategies for verification have emerged in the form of static analysis of programs (type checking, type inference, extended static checking, other properties of variables based on abstract interpretation) and model checking of computational structures (especially hardware), as well as software and hardware verification using automated theorem proving. Type inference, for instance, (with the types of program variables being weaker forms of invariants) is now widely considered a useful feature supported in many functional and logical languages such as ML.

However, the annotation burden remains, and the complication of automatically generating loop invariants is still unsolved. Below, we briefly review various attempts to deal with the problem.

The idea of expressing the values of variables as functions of loop counters, and then eliminating this auxiliary variables in order to get invariant formulas, was already at the core of the techniques in [EGLW72] and [KM76]. The main obstacles in the automatization of this approach were:

- finding a generic expression for the values of variables in loops with conditionals or nested loops was not normally possible.
- eliminating loop counters had to be done by hand.

Our method overcomes these difficulties by finding a generic expression not for all program states, but just for some of them in such a way that conditional
statements are handled correctly. Moreover, elimination theory provides us with the algorithmic tools to automate the elimination step.

In a different direction, in [Kar76] Karr gave an algorithm for finding invariant linear equalities at any program point. This work was extended by Cousot and Halbwachs [CH78], who applied the model of abstract interpretation (see [CC77]) to finding invariant linear inequalities. Like our techniques, both are based on forward propagation and fixed point computation (see [Weg75]). But whereas Karr obtained termination directly, Cousot and Halbwachs had to introduce a widening operator \( \Delta \), which computes an upper approximation of the set of states. Using the duality between ideals and varieties, our method can be regarded as computing also an upper approximation, which however is fine enough to guarantee completeness. Furthermore, the results that our techniques yield complement the linear inequalities obtained by means of these other methods.

From another standpoint, in [CSS03] Colón et al. have recently used constraint solving and quantifier elimination to attack the same problem of discovering invariant linear inequalities. Although we also have to eliminate variables in our approach, since we are dealing with polynomial equalities we can apply Gröbner bases and elimination theory, which are not as costly as the general methods for quantifier elimination such as cylindrical algebraic decomposition (CAD).

Another recent extension of Karr's ideas has been carried out by Müller-Olm and Seidl [M. 03], who find interprocedural polynomial equalities of bounded degree in programs with affine assignments. They use backward propagation and weakest preconditions, instead of forward propagation and strongest postconditions. When they can be applied, our techniques have the advantage that no bound on the degree is necessary; moreover, solvable mappings, which generalize affine mappings, are allowed in the assignments in our programming model.

## 2 Preliminaries

Given a field \( \mathbb{K} \), a mapping \( g : \mathbb{K}^r \to \mathbb{K}^r \) is said to be affine if it is of the form \( g(\vec{x}) = A\vec{x} + b \), where \( A \) is an \( s \times t \) matrix with coefficients in \( \mathbb{K} \), and \( b \in \mathbb{K}^s \).

We denote by \( \mathbb{K}[z] = \mathbb{K}[z_1, \ldots, z_l] \) the set of polynomials with coefficients in \( \mathbb{K} \) in the variables \( z_1, \ldots, z_l \). An ideal is a set \( I \subseteq \mathbb{K}[z] \) which is closed under addition and such that, if \( p \in \mathbb{K}[z] \) and \( q \in I \), then \( pq \in I \). Given a set of polynomials \( S \subseteq \mathbb{K}[z] \), the ideal spanned by \( S \) is

\[
\left\{ \sum_{j=1}^{k} p_j q_j \mid p_j \in \mathbb{K}[z], q_j \in S \right\}
\]

We denote it by \( \langle S \rangle_{\mathbb{K}[z]} \) or simply by \( \langle S \rangle \). The variety of \( S \) is defined as its set of zeroes, \( \forall(S) = \{ \bar{a} \in \mathbb{K}^l \mid p(\bar{a}) = 0 \ \forall p \in S \} \).

Reciprocally, if \( A \subseteq \mathbb{K}^r \) the ideal \( \mathbb{I}(A) = \{ p \in \mathbb{K}[z] \mid p(\bar{a}) = 0 \ \forall \bar{a} \in A \} \) is the annihilator of \( A \). If \( I \subseteq \mathbb{K}[z] \), we will write \( \mathbb{I}(\forall(I)) \) instead of \( \mathbb{I}(\forall(I)) \).
3 Programming Model

In this section we present our programming model; the domain of variables, the structure of loops and the expressions allowed in programs.

Let \( x_1, x_2, \ldots, x_m \) be the variables which change their value during the execution of the loop. We denote by \( \bar{x} \) the tuple of these variables. We restrict ourselves to just variables of rational type, because we need the properties of a field and also an exact representation in the implementation.

As regards loop structure, the only instructions we allow in loops are assignments and non-deterministic conditional statements. Moreover, programs are abstracted so that guards in loop headers and in conditionals are ignored. As assignments can be composed and nested conditionals can be merged, using the notation of Dijkstra’s guarded command language ([DiJ61]) we can assume that loops have the form:

```
while true do
  if true \rightarrow \bar{x} := f_1(\bar{x});
  \ldots
  \[ true \rightarrow \bar{x} := f_i(\bar{x});
  \ldots
  \[ true \rightarrow \bar{x} := f_n(\bar{x});
  end if
end while
```

where \( f_i : \mathbb{Q}^m \rightarrow \mathbb{Q}^m \) for \( 1 \leq i \leq n \).

It remains to determine the class of assignment mappings \( f_i \) that we are going to deal with. In order to do that, we introduce the concept of solvable polynomial mapping, which generalizes that of affine mapping. Intuitively, a solvable mapping \( g \) is a polynomial mapping such that the recurrence \( \bar{x}_{s+1} = g(\bar{x}_s) \) can be solved effectively and such that its solution (which is given by the general power \( g^s \)) has “polynomial structure”.

Before giving the formal definition we need some notation. Given \( U \subseteq \bar{x} \) a subset of the variables we denote by \( g_U : \mathbb{Q}^m \rightarrow \mathbb{Q}^{|U|} \) the mapping consisting in the (sorted) tuple of the \( j \)-th components of \( g \) such that \( x_j \in U \). For instance, for the mapping

\[
g(a, b, p, q) = (a - 1, b, p, q + b p)
\]

we would have

\[
g_{\{a\}}(a, b, p, q) = g_{\{a\}}(a) = a - 1
\]

\[
g_{\{a, b, p\}}(a, b, p, q) = g_{\{a, b, p\}}(a, b, p) = (a - 1, b, p)
\]

\[
g_{\{q\}}(a, b, p, q) = q + b p
\]

**Definition 1.** Let \( g \in \mathbb{Q}[\bar{x}]^m \) be a polynomial mapping. We say that \( g \) is solvable if there exists a partition of \( \bar{x} \), \( \bar{x} = U_1 \cup \cdots \cup U_k \), \( U_i \cap U_j = \emptyset \) if \( i \neq j \), such that \( \forall j : 1 \leq j \leq k \) we have

\[
g_{U_j}(\bar{x}) = M_j U_j^T + P_j(U_1, \ldots, U_{j-1})
\]
where \( M_j \in \mathbb{Q}[x_1, \ldots, x_k] \) is a matrix and \( P_j \) is a vector of \(|U_j|\) polynomials with coefficients in \( \mathbb{Q} \) and depending on the variables in \( U_1, \ldots, U_{j-1} \) (\( P_1 \) must necessarily be a constant vector).

Moreover, we define the eigenvalues of \( g \) as the union of the eigenvalues of the matrices \( M_j, 1 \leq j \leq k \).

Finally, an assignment \( \tilde{x} := g(\tilde{x}) \) is said to be solvable if the mapping \( g \) is solvable.

In our programming model, assignments have to be solvable.

Notice that any affine mapping \( g(\tilde{x}) = A\tilde{x} + b \) is solvable, since we can take \( U_1 = \tilde{x}, M_1 = A, P_1 = b \), and then the eigenvalues of \( g \) are the eigenvalues of \( A \).

Consider for example the following loop, which is an abstraction of a program that computes the product of two integer numbers:

\[
\langle x, y, z \rangle := \langle X, Y, 0 \rangle;
\]

while true do
  if \( \text{true} \) \( \rightarrow \langle x, y, z \rangle := \langle 2x, y/2 - 1/2, x + z \rangle; \)
  \[ \] true \( \rightarrow \langle x, y, z \rangle := \langle 2x, y/2, z \rangle; \)
end if
end while

The assignment mappings of the loop

\[
f_1(x, y, z) = (2x, y/2 - 1/2, x + z)
\]

\[
f_2(x, y, z) = (2x, y/2, z)
\]

are affine, and therefore solvable; in both cases the eigenvalues are \( \{2, 1/2, 1\} \).

Now let us consider an example of a solvable mapping which is not affine. For instance, the non-linear mapping

\[
g(a, b, p, q) = (a - 1, b, p, q + bp)
\]

is solvable. Indeed, we can take \( U_1 = \{a, b, p\}, M_1 = \text{diagonal}(1, 1, 1), P_1 = (-1, 0, 0) \), since

\[
g_{a,b,p}(a, b, p, q) = g(a, b, p)(a, b, p) = (a - 1, b, p)
\]

Then we can also take \( U_2 = \{q\} \), with \( M_2 = \{1\} \) and \( P_2 = bp \), as \( g_{\{q\}}(a, b, p, q) = q + bp \). Moreover, in this case the eigenvalues of \( g \) are just \( \{1\} \).

Therefore both assignments in the following loop, which is an abstraction of another program for the product of integer numbers, are solvable:

\[
\langle a, b, p, q \rangle := \langle A, B, 1, 0 \rangle;
\]

while true do
  if \( \text{true} \) \( \rightarrow \langle a, b, p, q \rangle := \langle a - 1, b, p, q + bp \rangle; \)
  \[ \] true \( \rightarrow \langle a, b, p, q \rangle := \langle a/2, b/2, 4p, q \rangle; \)
end if
end while

In order to motivate the name solvable, let us compute \( g' \). Equivalently, we can explicitly solve the recurrence equation

\[
(a_{s+1}, b_{s+1}, p_{s+1}, q_{s+1}) = g(a_s, b_s, p_s, q_s)
\]

whose solution is \( g'(a_0, b_0, p_0, q_0) \). We first solve the recurrence for \( a_s, b_s, p_s \):

\[
\begin{align*}
    a_{s+1} &= a_s - 1 \\
    b_{s+1} &= b_s \\
    p_{s+1} &= p_s
\end{align*}
\]

Then

\[
\begin{align*}
    a_s &= a_0 - s \\
    b_s &= b_0 \\
    p_s &= p_0
\end{align*}
\]

Now, as \( q_{s+1} = q_s + b_sp_s \), plugging in the expression for the variables that have already been solved we get the recurrence

\[
q_{s+1} = q_s + b_0p_0
\]

The solution of this equation is

\[
q_s = q_0 + b_0p_0s
\]

and thus

\[
g'(a, b, p, q) = (a - s, b, p, q + bps)
\]

Notice that, in this case, we have obtained a vector of polynomials in the program variables \( a, b, p \) and in the auxiliary variable \( s \).

4 Ideals of Invariant Polynomials

In this section we give the definition of invariant polynomials for the loops we are considering, and we also see that the algebraic structure of ideal is the natural object when studying them. We also link the concept to the work in [RCK] so as to get the theoretical background necessary to present the procedure properly.

Intuitively, an invariant polynomial is a polynomial which evaluates to 0 at any program state at the header of the loop. For example, in the loop

\[
\langle x, y, z \rangle := \langle X, Y, 0 \rangle;
\]

\textbf{while} true \textbf{do}

\textbf{if} true \textbf{then} \langle x, y, z \rangle := \langle 2x, y/2 - 1/2, x + z \rangle;

\textbf{else} \langle x, y, z \rangle := \langle 2x, y/2, z \rangle;

\textbf{end if}

\textbf{end while}
it can be seen that the polynomial \(z + xy - XY\) always yields 0 when evaluated at the loop header, and is therefore invariant.

In order to deal with variables which are initialized to parameters rather than to values in \(\mathbb{Q}\) (like in this case for \(x, y\)) or even uninitialized, our invariants will depend not only on variables \(\vec{x}\) representing the values of the variables at any iteration at the header of the loop, but also on variables \(\vec{x}^*\) standing for the initial values before entering the loop. If any of the variables is initialized to a rational value just before the loop, or more in general, if any polynomial equations are known to hold for the initial values of the variables, we can take \(I_0\) a set of such polynomials just in the \(\vec{x}^*\) variables to act as a precondition of the loop. For instance, in the example we could take \(I_0 = \{z^*\}\) (meaning that \(z = 0\) when we enter the loop), and our invariant polynomial would be rewritten as \(z + xy - z^*y^*\).

We need to introduce some notation before formally defining the notion of invariance for polynomials. Let us consider the set of strings over the alphabet \([n] = \{1, \ldots, n\}\), which we denote by \([n]^*\). We also write the tuple \(f_1, \ldots, f_n\) as \([f]\). For every string \(\sigma \in [n]^*\), we inductively define \([f]^\sigma\) as

\[
[f]^\lambda(\vec{x}) = \vec{x}, \quad [f]^\sigma(i)(\vec{x}) = f_i([f]^\sigma(\vec{x}))
\]

where \(\lambda\) denotes the empty string. Each \(\sigma \in [n]^*\) represents an execution path, and \([f]^\sigma\) maps initial states of the variables to states after executing the path \(\sigma\).

Now we are in condition to define invariant polynomials:

**Definition 2.** Given a set \(I_0 \subseteq \mathbb{Q}[\vec{x}^*]\), a polynomial \(p \in \mathbb{Q}[\vec{x}, \vec{x}^*]\) is invariant with respect to \(I_0\) if \(\forall \vec{x}^* \in \mathbb{V}(I_0) \forall \vec{\sigma} \in [n]^*, \; p([f]^{\vec{\sigma}}(\vec{x}^*), \vec{x}^*) = 0\).

Notice that, if the polynomial \(p\) is invariant with respect to \(I_0\), then it is invariant with respect to \(\langle I_0 \rangle\), as \(\mathbb{V}(I_0) = \mathbb{V}(\langle I_0 \rangle)\). So we can assume that \(I_0\) is always an ideal.

The following result shows that the set of all polynomial invariants with respect to a given \(I_0\) is an ideal:

**Proposition 1.** Given an ideal \(I_0 \subseteq \mathbb{Q}[\vec{x}^*]\),

\[
P_\infty := \bigcap_{\sigma \in [n]^*} \left\{ p \in \mathbb{Q}[\vec{x}, \vec{x}^*] \mid \forall \vec{x}^* \in \mathbb{V}(I_0) \; p([f]^{\vec{\sigma}}(\vec{x}^*), \vec{x}^*) = 0 \right\}
\]

is an ideal.

**Proof.** It is evident that the addition of two polynomials in \(P_\infty\) is in \(P_\infty\), and that the product of an arbitrary polynomial by a polynomial in \(P_\infty\) is in \(P_\infty\) as well. Therefore \(P_\infty\) is an ideal.

\(\square\)

We will refer to this ideal as the *invariant ideal* of the loop.

In the example, we have that \(z + xy - x^*y^*\) is invariant with respect to \(I_0 = \langle z^* \rangle\); and moreover, we will see later on that \(P_\infty = \langle z + xy - x^*y^* \rangle\).
Our next goal is to show the relationship between invariant polynomials and invariant conjunctions of polynomial equalities, i.e. formulas of the form

$$\bigwedge_{p \in P} p(\bar{x}, \bar{x}^*) = 0$$

where $P \subseteq \mathbb{Q}[\bar{x}, \bar{x}^*]$ is finite. We denote by $\mathcal{P}$ the set of all such formulas.

First of all, we need to define the notion of invariance in $\mathcal{P}$ according to the ideas in [RCK]:

**Definition 3.** Let $I_0 \subseteq \mathbb{Q}[\bar{x}^*]$ be an ideal of polynomials satisfied by the initial values. A formula $R \in \mathcal{P}$ is $\mathcal{P}$-invariant with respect to $I_0$ if:

i) $\forall \bar{a}^* \in \forall (I_0), R(\bar{a}^*, \bar{a}^*)$ holds.

ii) $\forall i : 1 \leq i \leq n, R(\bar{x}, \bar{x}^*) \Rightarrow R(f_i(\bar{x}), \bar{x}^*)$.

We want to prove that, if we take any finite basis of $P_\infty$ (whose existence is guaranteed by Hilbert’s basis theorem), equate its polynomials to 0 and finally conjunct the resulting equations, we get a formula which is $\mathcal{P}$-invariant and, moreover, it is the strongest among all $\mathcal{P}$-invariant formulas. In order to do so, we need the following lemma:

**Lemma 1.** If $R$ is $\mathcal{P}$-invariant with respect to an ideal $I_0$, then $\forall \bar{a}^* \in \forall (I_0)$ $\forall \sigma \in [n]^* R([f]^{\sigma}(\bar{a}^*), \bar{a}^*)$ holds.

**Proof.** By induction over the length of $\sigma$. If $|\sigma| = 0$ then $\sigma = \lambda$, and $\forall \bar{a}^* \in \forall (I_0)$ by $\mathcal{P}$-invariance we have that $R([f]^{\lambda}(\bar{a}^*), \bar{a}^*) \equiv R(\bar{a}^*, \bar{a}^*)$ holds.

Now, if $|\sigma| > 0 \exists i : 1 \leq i \leq n \exists \sigma' \in [n]^*$ such that $\sigma = \sigma' \cdot i$. Thus, by induction hypothesis $\forall \bar{a}^* \in \forall (I_0) R([f]^{\sigma'}(\bar{a}^*), \bar{a}^*)$ holds, and by $\mathcal{P}$-invariance,

$$R([f]^{\sigma'}(\bar{a}^*), \bar{a}^*) \Rightarrow R(f_i([f]^{\sigma'}(\bar{a}^*)), \bar{a}^*) \equiv R([f]^{\sigma'}(\bar{a}^*), \bar{a}^*) \equiv R([f]^{\sigma}(\bar{a}^*), \bar{a}^*)$$

$\square$

Now we can link invariance for polynomials and $\mathcal{P}$-invariance for formulas, which in the next section will allow us to apply all the procedure presented in [RCK] to compute $P_\infty$:

**Lemma 2.** Given $I_0 \subseteq \mathbb{Q}[\bar{x}^*]$, let $B$ a finite basis of $P_\infty$ and let

$$R_\infty := (\bigwedge_{p \in B} p = 0) \in \mathcal{P}$$

Then $R_\infty$ satisfies:

i) $R_\infty$ is $\mathcal{P}$-invariant

ii) $\forall R \mathcal{P}$-invariant, $R_\infty(\bar{x}, \bar{x}^*) \Rightarrow R(\bar{x}, \bar{x}^*)$
Proof. First, let us prove i). Let us prove that $\forall \bar{a}^* \in \forall (I_0) \ R_\infty (\bar{a}^*, \bar{a}^*)$ holds. Indeed, $\forall p \in B \subseteq P_\infty \ \forall \bar{a}^* \in \forall (I_0)$ taking $\sigma = \lambda$ we have $0 = p([f^\lambda (\bar{a}^*), \bar{a}^*]) = p(\bar{a}^*, \bar{a}^*)$. So $\forall \bar{a}^* \in \forall (I_0) \ \forall p \in B \ p(\bar{a}^*, \bar{a}^*) = 0$ and $R_\infty (\bar{a}^*, \bar{a}^*)$ is true.

Now let us prove that $\forall i : 1 \leq i \leq n, R_\infty (\bar{x}, \bar{z}^*) \Rightarrow R_\infty (f_i(\bar{x}), \bar{z}^*)$. Let us fix $i : 1 \leq i \leq n$ and take $\bar{a}, \bar{a}^* \in \mathbb{Q}^m$ such that $R_\infty (\bar{a}, \bar{a}^*)$ holds. Then $(\bar{a}, \bar{a}^*) \in \forall (B) = \forall (P_\infty)$.

Moreover, if $p(\bar{x}, \bar{z}^*) \in P_\infty$ then $p(f_i(\bar{x}), \bar{z}^*) \in P_\infty$, as $\forall \sigma \in [n]^*$

$$p(f_i([f^\sigma (\bar{x})]), \bar{z}^*) = p([f]^{\sigma, i}(\bar{x}), \bar{z}^*)$$

So $\forall p \in B \ p(f_i(\bar{x}), \bar{z}^*) \in P_\infty$. Since $(\bar{a}, \bar{a}^*) \in \forall (P_\infty)$, $\forall p \in B \ p(f_i(\bar{a}), \bar{a}^*) = 0$, and $R(f_i(\bar{a}), \bar{a}^*)$ holds.

Secondly, let us prove ii). Let $R$ be a $P$-invariant formula. Then by Lemma 1, $\forall \bar{a}^* \in \forall (I_0) \ \forall \sigma \in [n]^* \ R([f^\sigma (\bar{a}^*), \bar{a}^*])$ holds. So if $q(\bar{x}, \bar{z}^*) = 0$ is one of the atomic formulas in $R$, $q([f]^\sigma (\bar{a}^*), \bar{a}^*) = 0$. Therefore $q \in P_\infty$.

Now let us see that $R_\infty (\bar{x}, \bar{z}^*) \Rightarrow R(\bar{x}, \bar{z}^*)$. If $\bar{a}, \bar{a}^* \in \mathbb{Q}^m$ are such that $R_\infty (\bar{a}, \bar{a}^*)$ is true, then $(\bar{a}, \bar{a}^*) \in \forall (B) = \forall (P_\infty)$; but as $\forall q$ such that $q = 0$ is an atomic formula of $R$ we have $q \in P_\infty$, then $q(\bar{a}, \bar{a}^*) = 0$ and finally $R(\bar{a}, \bar{a}^*)$ holds.

$\square$

5 The procedure for finding polynomial invariants

In this section we describe a fixed point procedure which, given the mappings of the assignments $f_1, \ldots, f_n$ and an ideal $I_0$ of polynomials satisfied by the initial values, on termination returns the invariant ideal $P_\infty$.

Before showing this procedure, we need more terminology. Given a polynomial mapping $f \in \mathbb{Q}[[\bar{z}]]^m$, we say that it is (polynomially) invertible if $\exists f^{-1} \in \mathbb{Q}[[\bar{z}]]^m$. Moreover, given a polynomial mapping $g \in \mathbb{Q}[[\bar{x}, \bar{z}]]$, where the $\bar{z}$ are auxiliary variables, and an ideal $I \subseteq \mathbb{Q}[[\bar{x}, \bar{z}]]$ we define the ideal in $\mathbb{Q}[[\bar{z}, \bar{z}^*]]$

$$\text{subs}(g, I) = \langle \{p(g(\bar{z}, \bar{z}^*), \bar{z}^*) \in \mathbb{Q}[[\bar{z}, \bar{z}^*] \mid p(\bar{x}, \bar{z}^*) \in I]\rangle_{\mathbb{Q}[[\bar{z}, \bar{z}^*]}}$$

In particular, it can be easily proved that if $g \in \mathbb{Q}[[\bar{z}]]^m$ is an invertible polynomial mapping (notice that there are no auxiliary variables in this case), then $\text{subs}(g, I) \subseteq \mathbb{Q}[[\bar{z}, \bar{z}^*]]$,

$$\text{subs}(g, I) = \{p(g(\bar{z}), \bar{z}^*) \in \mathbb{Q}[[\bar{z}, \bar{z}^*] \mid p(\bar{x}, \bar{z}^*) \in I]\}$$

and $p(\bar{x}, \bar{z}^*) \subseteq \text{subs}(g, I)$ if and only if $p(g^{-1}(\bar{x}), \bar{z}^*) \subseteq I$.

For technical reasons, we need that the $f_i$’s are solvable and invertible mappings. We also require that $I_0$ satisfies $I_0 = \forall (I_0)$. The procedure is then as follows:

Input.
The invertible solvable mappings $f_1, \ldots, f_n$ of the assignments
An ideal $I_0$ of polynomials satisfied by the initial values such that
\[ I_0 = \exists V(I_0) \]

**Output.**

The invariant ideal \( P_\infty \)

var \( I', I : \) ideals in \( \mathbb{Q}[\tilde{x}, \tilde{x}^*] \) end var

\[ I' := \mathbb{Q}[\tilde{x}, \tilde{x}^*] \]
\[ I := \{ t_1 - t_1', ..., t_m - t_m' \} \cup I_0 \]
while \( I' \neq I \) do
\[ I' := I \]
\[ I := \bigcap_{i=0}^{\infty} \bigcap_{i=1}^{n} \text{subs}(f_i^{-s}, I) \]
end while

return \( I \)

We remark that, since the \( f_i \)'s are invertible, the \( f_i^{-s} \)'s are polynomial mappings for any \( s \in \mathbb{Z} \).

The following theorem ensures that on termination the result, i.e., the ideal stored in the variable \( I \), is correct, in the sense that all polynomials contained in it are invariant for the loop, and complete, in the sense that it contains the whole invariant ideal:

**Theorem 1.** If the procedure terminates, \( I = P_\infty \).

The theorem is a direct consequence of the results presented in [RCK]. In this paper, an abstract procedure in terms of formulas is given, which after instantiation for the case of conjunctions of polynomial equalities yields the above procedure (see also Section 7.2 for some necessary lemmata).

### 5.1 Termination of the procedure

The above procedure is shown to terminate under two cases:

- if the assignment mappings \( f_i \)'s are solvable and commute, i.e., \( f_i \circ f_j = f_j \circ f_i \) for \( 1 \leq i, j \leq n \). In that case, it is shown that the procedure terminates in at most \( n + 1 \) iterations, where \( n \) is the number of branches in the body of the loop.
- if the assignment mappings \( f_i \)'s are solvable and the associated eigenvalues are positive. In that case, it can be proved that the procedure terminates in at most \( 2m + 1 \) iterations, where \( m \) is the number of variables changing their value in the body of the loop.

In the rest of this section we will focus on the first proposition. The second is proved in detail in Section 7.

We first prove a more general result, namely, that at the \( N \)-th iteration of the procedure, the effect of all possible compositions of assignments with \( \leq N - 1 \) twists has been considered. Using this general result we show that, if the assignment mappings commute, then a fixed point is reached in \( n + 1 \) iterations,
where \( n \) is the number of branches in the conditional statement of the body of the loop. In particular, if \( n = 1 \), i.e. there are no conditional statements, the procedure takes at most 2 iterations to terminate.

First of all, we need to introduce some notation. Given \( \sigma \in [n]^* \) we define \( \nu(\sigma) \), the number of alternations of \( \sigma \) as:

- \( \nu(\lambda) = -1 \) (\( \lambda \) is the empty string)
- \( \nu(\epsilon) = 0 \)
- \( \nu(i, j, \sigma) = \nu(j, \sigma) \) if \( i = j \)
- \( \nu(i, j, \sigma) = 1 + \nu(j, \sigma) \) if \( i \neq j \)
- \( 1 \leq i, j \leq n \)

Moreover, for \( N \in \mathbb{N} \) we also define \( \mathcal{Z}_N \) as the ideal stored in the variable \( I \) in the procedure at the end of the \( N \)-th iteration.

Then we have the following lemma:

**Lemma 3.** \( \forall N \in \mathbb{N} \)

\[
\mathcal{Z}_N = \bigcap_{\nu(\sigma) \leq N} \text{subs}((|f|^{\sigma})^{-1}, \mathcal{Z}_0)
\]

**Proof.** Let us prove it by induction on \( N \). If \( N = 0 \), then the only \( \sigma \in [n]^* \) such that \( \nu(\sigma) \leq -1 \) is \( \sigma = \lambda \), the empty string. Since \( \text{subs}((|f|^{\lambda})^{-1}, \mathcal{Z}_0) = \mathcal{Z}_0 \), our claim is true.

Now let us assume that \( N > 0 \). By definition of \( \mathcal{Z}_N \),

\[
\mathcal{Z}_N = \bigcap_{i=1}^{n} \bigcap_{j=0}^{\infty} \text{subs}(f_i^{-j}, \mathcal{Z}_{N-1})
\]

Applying the induction hypothesis,

\[
\mathcal{Z}_N = \bigcap_{i=1}^{n} \bigcap_{j=0}^{\infty} \text{subs}(f_i^{-j}, \bigcap_{\nu(\sigma) \leq N-2} \text{subs}((|f|^{\sigma})^{-1}, \mathcal{Z}_0))
\]

As the mappings \( f_i^{-j} \) are invertible, it can be proved that \( \text{subs} \) distributes with respect to \( \cap \). Then

\[
\mathcal{Z}_N = \bigcap_{i=1}^{n} \bigcap_{j=0}^{\infty} \text{subs}(f_i^{-j}, \text{subs}((|f|^{\sigma})^{-1}, \mathcal{Z}_0))
\]

Given \( f, g \in \mathbb{Q}[\mathbb{Z}]^m \) and an ideal \( I \subseteq \mathbb{Q}[\mathbb{Z}] \), \( \text{subs}(f, \text{subs}(g, I)) = \text{subs}(g \circ f, I) \).
So

\[
\mathcal{Z}_N = \bigcap_{i=1}^{n} \bigcap_{j=0}^{\infty} \text{subs}((|f|^{\sigma})^{-1} \circ (f_i^{-j})^{-1}, \mathcal{Z}_0) =
\]
\[
\left( \bigcap_{i=1}^{n+1} \bigcap_{\sigma \in [n]^*} \bigcap_{\nu(\sigma) \leq n-2} \text{subs}(([f]^{ \nu(\sigma)} \circ [f]^{\tau})^{-1}, \mathcal{Z}_0) \right) = \\
\left( \bigcap_{i=1}^{n+1} \bigcap_{\sigma \in [n]^*} \bigcap_{\nu(\sigma) \leq n-2} \text{subs}(([f]^{\nu(\sigma)} \circ [f]^{\tau})^{-1}, \mathcal{Z}_0) \right) = \\
\bigcap_{\sigma \in [n]^*} \bigcap_{\nu(\sigma) \leq n-1} \text{subs}(([f]^{\nu(\sigma)})^{-1}, \mathcal{Z}_0)
\]

which is what we wanted to show.

\[\Box\]

Finally, we have the result of termination if the mappings \( f_i \) commute:

**Theorem 2.** If the mappings \( f_i \) commute, i.e. \( f_i \circ f_j = f_j \circ f_i \) \( \forall i, j : 1 \leq i, j \leq n \), then the procedure terminates in at most \( n + 1 \) iterations.

**Proof.** If the \( f_i \)'s commute then \( \forall \sigma \in [n]^* \) we can build, by rearranging the mappings \( f_i \) and collapsing them in a single power, \( \tau \in [n]^* \) such that \( \nu(\tau) \leq n-1 \) and \( [f]^{\tau} = [f]^{\rho} \). Then, by Lemma 3

\[
\mathcal{Z}_{n+1} = \bigcap_{\sigma \in [n]^*} \left( \text{subs}(([f]^{\nu(\sigma)})^{-1}, \mathcal{Z}_0) \right) = \\
\bigcap_{\sigma \in [n]^*} \left( \text{subs}(([f]^{\nu(\sigma)})^{-1}, \mathcal{Z}_0) \right) = \mathcal{Z}_n
\]

Therefore the procedure terminates in at most \( n + 1 \) iterations.

\[\Box\]

### 5.2 Behaviour of the procedure in relation to program states

In order to understand better the procedure, in this section we show that, at the end of the \( N \)-th iteration, the ideal stored in the variable \( I, \mathcal{Z}_N \), is the ideal of the polynomials that evaluate to 0 for all those program states whose path has a number of alternations \( \leq N - 1 \).

By definition

\[
P_\infty = \bigcap_{\sigma \in [n]^*} \left\{ p \in \mathbb{Q}[\bar{x}, \bar{x}^*] \mid \forall \bar{a}^* \in \mathbb{V}(I_0) \ p([f]^{\nu(\bar{a}^*)} \circ \bar{a}^*) = 0 \right\}
\]

Given \( \sigma \in [n]^* \), the ideal

\[
\{ p \in \mathbb{Q}[\bar{x}, \bar{x}^*] \mid \forall \bar{a}^* \in \mathbb{V}(I_0) \ p([f]^{\nu(\bar{a}^*)} \circ \bar{a}^*) = 0 \}
\]
are those polynomials that evaluate to 0 at any program state with execution path $\sigma$. $P_\infty$ is the infinite intersection of these ideals for all execution paths. In particular, we can consider $P_\infty$ as the “limit” of the ideals $P_N$, where we define

$$P_N := \bigcap_{\sigma \in [n]^*, \nu(\sigma) \leq N} \left\{ p \in \mathbb{Q}\{\bar{x}, \bar{x}^*\} \mid \forall \bar{\alpha}^* \in \bigvee(I_0) \, p([f]^\sigma(\bar{\alpha}^*), \bar{\alpha}^*) = 0 \right\}$$

Intuitively, $P_N$ is the ideal of those polynomials that evaluate to 0 for all the program states whose execution paths have $\leq N$ alternations.

We have the following result:

**Proposition 2.** $\forall N \in \mathbb{N}, \exists_N = P_{N-1}$.

**Proof.** By Lemma 3, $\forall N \in \mathbb{N}$

$$\exists_N = \bigcap_{\sigma \in [n]^*, \nu(\sigma) \leq N-1} \text{subs}(([f]^\sigma)^{-1}, \exists_0)$$

First, let us prove $\exists_N \subseteq P_{N-1}$. Let $p \in \exists_N$. If $\sigma \in [n]^*$ is such that $\nu(\sigma) \leq N - 1$, then $p \in \text{subs}(([f]^\sigma)^{-1}, \exists_0)$, or equivalently, $p([f]^\sigma(\bar{x}), \bar{x}^*) \in \exists_0$. Since $\exists_0 = \langle \{x_1 - x_1^*, \ldots, x_m - x_m^*\} \cup I_0 \rangle$, there exist certain polynomials $r_i \in I_0$ and $q_i, p_j \in \mathbb{Q}\{\bar{x}, \bar{x}^*\}$ ($1 \leq i \leq k, 1 \leq j \leq m$) such that

$$p([f]^\sigma(\bar{x}), \bar{x}^*) = \sum_{i=1}^{k} q_i(\bar{x}, \bar{x}^*) r_i(\bar{x}^*) + \sum_{j=1}^{m} p_j(\bar{x}, \bar{x}^*)(x_j - x_j^*)$$

Now, if we take any $\bar{\alpha}^* \in \bigvee(I_0)$, it is clear that $p([f]^\sigma(\bar{\alpha}^*), \bar{\alpha}^*) = 0$. Therefore $\exists_N \subseteq P_{N-1}$.

Secondly, let us prove $\exists_N \supseteq P_{N-1}$. Let $p \in P_{N-1}$. We have to see that $\forall \sigma \in [n]^*$ such that $\nu(\sigma) \leq N - 1$, $p \in \text{subs}(([f]^\sigma)^{-1}, \exists_0)$, or equivalently $p([f]^\sigma(\bar{x}), \bar{x}^*) \in \exists_0$. By Lemma 11 in Section 7.2, as $p \in P_{N-1}$ and

$$\forall \left( \left( \bigcup_{j=1}^{m} \{x_j - x_j^*\} \right) \cup I_0 \right) = \{ (\bar{\alpha}^*, \bar{\alpha}^*) \in \mathbb{Q}\{\bar{x}, \bar{x}^*\} \mid \bar{\alpha}^* \in \bigvee(I_0) \}$$

we have

$$p([f]^\sigma(\bar{x}), \bar{x}^*) \in \bigvee \left( \left( \bigcup_{j=1}^{m} \{x_j - x_j^*\} \right) \cup I_0 \right) = \bigvee \left( \bigcup_{j=1}^{m} \{x_j - x_j^*\} \cup I_0 \right) = \exists_0$$

Therefore, at the end of the $N$-th iteration the procedure has computed the ideal of the polynomials common for all those paths with $\leq N - 1$ alternations. For two branches in the body of the loop ($n = 2$), the following diagram illustrates the paths that at each iteration the procedure intersects. The nodes
the tree are program states, and the root represents initial states. At a given node, the left arc means taking \( \tilde{x} := f_1(\tilde{x}) \), and the right arc means taking \( \tilde{x} := f_2(\tilde{x}) \). If two paths have some arc in common, we have drawn the thickness corresponding to the one with less number of alternations.

6 Approximating the Infinite Intersection with Gröbner Bases

In this section, we show how the procedure can be implemented with Gröbner bases and elimination theory. We also prove that the approximations performed are fine enough to guarantee that we do not lose completeness.

The problem with the procedure as given in Section 5 is that the assignment

\[
I := \bigcap_{s=0}^{\infty} \bigcap_{i=1}^{n} \text{subs}(f_i^{s-1}, I)
\]

is not directly implementable, due to the infinite intersection.

We overcome this hurdle as follows. We consider the parameter \( s \) as a new variable and compute the general expression of the powers \( f_i^{s-1} \) for \( 1 \leq i \leq n \); for this reason we need the mappings \( f_i \) to be invertible and solvable. For the time being, let us assume that \( f_i^{s-1}(\tilde{x}) \in \mathbb{Q}[s, \tilde{x}] \). Then, given a basis for \( I \subseteq \mathbb{Q}[\tilde{x}, \tilde{x}^*] \), we get a basis for \( \text{subs}(f_i^{s-1}, I) \subseteq \mathbb{Q}[s, \tilde{x}, \tilde{x}^*] \) by substituting the \( \tilde{x} \) variables by \( f_i^{s-1}(\tilde{x}) \). By means of Gröbner bases, the finite intersection \( \bigcap_{s=1}^{n} \text{subs}(f_i^{s-1}, I) \) can be computed. What remains to be done is the infinite intersection. The approximation consists in taking an elimination monomial order for \( s \) and then eliminate this auxiliary variable from \( \bigcap_{s=1}^{n} \text{subs}(f_i^{s-1}, I) \).

Nevertheless, there is yet another difficulty with this approach. The hypothesis \( f_i^{s-1}(\tilde{x}) \) \( \in \mathbb{Q}[s, \tilde{x}] \) does not necessarily hold in general; exponential terms might appear, like in the first example from Section 3:

\[
\langle x, y, z \rangle := \langle X, Y, 0 \rangle;
\]

\[\textbf{while} \, \text{true} \, \textbf{do} \]

\[\text{if} \, \text{true} \rightarrow \langle x, y, z \rangle := \langle 2x, y/2 - 1/2, x + z \rangle;\]

\[\text{if} \, \text{false} \rightarrow \langle x, y, z \rangle := \langle 2x, y/2, z \rangle;\]

\[\textbf{end if} \]

\[\textbf{end while} \]

\( f_1(x, y, z) = (2x, y/2 - 1/2, x + z) \)
\[ f_2(x, y, z) = (2x, y/2, z) \]
\[ f_1^1(x, y, z) = (2^t x, (1/2)^t y + (1/2)^t - 1, z + (2^t - 1)x) \]
\[ f_2^1(x, y, z) = (2^t x, (1/2)^t y, z) \]

In this case the eigenvalues of the \( f_i \)'s are \( \{1/2, 2, 1\} \).

Notice that, however, \( f_1^1(x, y, z) \) and \( f_2^1(x, y, z) \) have “polynomial structure”,
in the sense that they are linear combinations of polynomials and exponentials.
In general, we have the following result concerning the powers of solvable mappings:

**Theorem 3.** Let \( g \in \mathbb{Q}[\bar{x}]^m \) be a solvable mapping with rational eigenvalues.
Then for \( 1 \leq j \leq m \) \( g_j^l(\bar{x}) \), the \( j \)-th component of \( g^l(\bar{x}) \), can be expressed as

\[ g_j^l(\bar{x}) = \sum_{i=1}^{k_j} P_{ji}(s, \bar{x})(\gamma_{ji})^l, \quad 1 \leq j \leq m, \quad s \geq 0 \]

where for \( 1 \leq j \leq m, 1 \leq l \leq k_j, P_{ji} \in \mathbb{Q}[s, \bar{x}] \) and \( \gamma_{ji} \in \mathbb{Q} \). Moreover, the \( \gamma_{ji} \) are products of the eigenvalues of \( g \).

The proof (see Appendix A) is based on the fact that a matrix \( M \in \mathbb{Q}^{n \times r} \)
with rational eigenvalues can be decomposed as \( M = S^{-1}JS \), with \( S, J \in \mathbb{Q}^{n \times r} \),
\( \det(S) \neq 0 \) and \( J \) the Jordan normal form of \( M \) ([Nom66]); and also on the fact
that a sequence \( (w_s)_{s \in \mathbb{N}} \) is of the form

\[ w_s = \sum_{i=1}^{k} P_i(s)(\gamma_i)^s, \quad s \geq 0 \]

with the \( P_i \)'s polynomials for \( 1 \leq l \leq k \) if and only if its generating function
\( W(z) = \sum_{s=0}^{\infty} w_s z^s \) is a rational function (see [Sta97] for an introduction to generating functions).

A way to sort this problem out is to introduce more auxiliary variables to replace
the exponential terms \( \gamma_{ji} \) and then eliminate them with a suitable elimination order.
From now on in this section let us assume that \( \mathcal{U}_{i=1}^{n_i} \) eigenvalues \( (f_i) \subseteq \mathbb{Q}^+ \).
Notice that termination is guaranteed in this case, see Section 5.1; moreover, Lemma 15 in Section 7.3 shows that this condition is sufficient to ensure that the \( f_i \)'s are invertible mappings.

It is clear that \( \forall \gamma \in \mathbb{Q}^+ \) there exists a unique prime decomposition of the form \( \gamma = \prod_{i=1}^{k} \lambda_i^{\alpha_i} \), where the \( \lambda_i \)'s are primes and \( \alpha_i \in \mathbb{Z} \) for \( 1 \leq i \leq k \). So we can compute a “base” \( A = \{ \lambda_1, \ldots, \lambda_k \} \subseteq \mathbb{N} \) of prime numbers such that
\( \forall \gamma \in \mathcal{U}_{i=1}^{n_i} \) eigenvalues \( (f_i) \) we have \( \gamma = \prod_{i=1}^{k} \lambda_i^{\alpha_i} \) for certain \( \alpha_i \in \mathbb{Z} \). Then

\[ \gamma^s = \prod_{i=1}^{k} (\lambda_i^{\alpha_i})^s = \prod_{i=1}^{k} (\lambda_i^s \text{sign} (\alpha_i))^{\left| \alpha_i \right|} \]

Now we can introduce the variable \( u_i \) to replace \( \lambda_i^s \) and the variable \( v_i \) to replace \( \lambda_i^{-s} \). By Theorem 3 for \( 1 \leq i \leq n \) there exists a polynomial mapping
\( F_i = F_i(s, \bar{u}, \bar{v}, \bar{x}) : \mathbb{Q}^{1+2k+m} \rightarrow \mathbb{Q}^m \) such that \( \forall t \in \mathbb{N}, \)

\[ f_i^t(\bar{x}) = F_i(t, \lambda_i^t, \lambda_i^{-t}, \bar{x}) \]
and

\[ f_i^{-1}(\hat{x}) = F_i(-t, \hat{\lambda}^{-t}, \lambda^t, \hat{x}) \]

where \( \lambda^t = (\lambda_1^t, \ldots, \lambda_k^t) \).

For instance, in our previous example we can take \( A = \{2\} \) and then we have:

\[
\begin{align*}
    f_1(x, y, z) &= (2x, y/2 - 1/2, x + z) \\
    f_2(x, y, z) &= (2x, y/2, z) \\
    f_1^t(x, y, z) &= (2^t x, (1/2)^t y + (1/2)^t - 1, z + (2^t - 1)x) \\
    f_2^t(x, y, z) &= (2^t x, (1/2)^t y, z) \\
    F_1(s, u, v, x, y, z) &= (ux, vy + v - 1, z + (u - 1)x) \\
    F_2(s, u, v, x, y, z) &= (ux, vy, z)
\end{align*}
\]

where the variables \( u, v \) represent \( 2^t \) and \( (1/2)^t \) respectively.

So far we have not considered the possible polynomial relations between \( t \), the \( \lambda_i^t \)'s and the \( \lambda_i^{-t} \)'s, which may be important in order to eliminate the auxiliary variables. Let \( L = \{ t \in \mathbb{Q}[\bar{u}, \bar{v}] \mid l(t, \bar{X}, \bar{\lambda}) = 0 \ \forall t \in \mathbb{N} \} \) be this set of polynomials. Let us also define \( L = \{ u_1v_1 - 1, \ldots, u_kv_k - 1 \} \). Then it can be shown that \( \langle L \rangle_{\mathbb{Q}[u, v, r]} = L \) (see Appendix B for the proof), and therefore we have a precise characterization of \( L \).

For instance, since in the example we have \( A = \{2\} \) and the variables \( u, v \) represent \( 2^t \) and \( (1/2)^t \) respectively, in this case \( L = \{uv - 1\} \).

### 6.1 Implementation

In the implementation of the procedure, the operations between ideals have been replaced by operations between sets of polynomials, identifying sets of polynomials with the ideals they generate:

**Input.**

The solvable mappings with positive rational eigenvalues \( f_1, \ldots, f_n \) of the assignments

A set \( S_0 \) of polynomials satisfied by the initial values such that

\[ \langle S_0 \rangle = \mathbb{V}(\langle S_0 \rangle) \]

**Output.**

A finite basis for the invariant ideal \( P_\infty \)

\[
\begin{align*}
    &\text{var}\quad S^t, S : \text{sets of polynomials in } \mathbb{Q}[\bar{x}, \bar{x}^*] \\
    &\quad S_{aux} : \text{set of polynomials in } \mathbb{Q}[s, \bar{u}, \bar{v}, \bar{z}, \bar{x}^*] \\
\end{align*}
\]

**end var**

1: compute \( f_1^t, \ldots, f_n^t, F_1, \ldots, F_n, L \)
2: \( S^t := \{1\} \)
3: \( S := \text{Gröbner basis}(\{x_1 - x_1^*, \ldots, x_m - x_m^*\} \cup S_0, \text{typ}) \)
4: while $S' \neq S$ do
5: \ 
6: $S_{aux} := \text{gröbner basis}(\bigcap_{i=1}^{n}(\text{subs}(F_i(-s, \tilde{v}, \tilde{u}, \cdot), S)_{q[x, z, z^*, z^*]}, >))$
7: $S_{aux} := \text{gröbner basis}(S_{aux} \cup L, \succ)$
8: $S := \{ \text{polynomials in } S_{aux} \text{ without } s, \tilde{u}, \tilde{v} \}$
9: end while
10: return $S$

At line 1, the $f_i$’s are computed by means of linear algebra or generating functions, using partial fraction decomposition. For computing the $F_i$’s from the $f_i$’s, the eigenvalues of the $f_i$’s are factorized and auxiliary variables $\tilde{u}$ and $\tilde{v}$ are introduced to replace the exponentials. All this can be done efficiently using commands supported in most mathematical packages, like $\text{rsolve}$ in Maple for solving recurrences.

At line 3, the function $\text{gröbner basis}$ computes the reduced Gröbner basis of the ideal generated by a set of polynomials with respect to a specified monomial order. In this case, the order $\succ$ is the same as at line 7. The requirements on it are explained below.

The function $\text{subs}$ at line 6 substitutes the $\tilde{x}$ variables in the polynomials of the second argument by the polynomials in the first argument; this is the way the function $\text{subs}$ for ideals is implemented. The intersection of ideals at the same line is performed by using Gröbner bases methods. In this case, the monomial ordering $\succ$ used in the computation of the Gröbner basis is arbitrary.

At line 7, the order $\succ$ on monomials, which is the same as at line 3, is chosen to eliminate the variables $s, \tilde{u}, \tilde{v}$ (typically using block-order or lexicographic ordering).

At line 8, polynomials not containing any of the auxiliary variables $s, \tilde{u}, \tilde{v}$ are selected from the Gröbner basis, so that the result on termination of the algorithm is a set of polynomials $S$ such that

$$\langle S \rangle_{q[x, z^*]} = \mathbb{Q}[\tilde{x}, z^*] \cap \left( L \cup \left( \bigcap_{i=1}^{n} \text{subs}(F_i(-s, \tilde{v}, \tilde{u}, \cdot), \langle S \rangle)_{q[x, z, z^*, z^*]} \right) \right)$$

Finally, the equality test on ideals is implemented at line 4 by comparing reduced Gröbner bases with respect to the same ordering, since every ideal has a unique reduced Gröbner basis once the ordering is fixed. Namely, both $S$ and $S'$ are always the reduced Gröbner bases of their corresponding ideals with respect to $\succ$.

The following result ensures that the above implementation is still correct and complete:

**Theorem 4.** If the procedure terminates with output $I^*$, the implementation terminates in at most the same number of iterations with output $S^*$ such that $\langle S^* \rangle_{q[x, z^*]} = I^*$.

See Appendix C. The proof is based on two facts: i) $P_\infty \subseteq \langle S \rangle$ is kept invariant during all the execution, and so, in particular, on termination $P_\infty \subseteq$
\(\langle S^*\rangle\); and ii), at any iteration, the ideal \(I\) computed by the procedure includes the ideal \(\langle S\rangle\) generated by the polynomials obtained in the implementation. So, if the procedure terminates, we have \(I^* = P_\infty \subseteq \langle S^*\rangle \subseteq I^*\). Therefore all inclusions are in fact equalities, and the implementation terminates with a set of polynomials generating \(P_\infty\) in at most the same number of steps as the procedure.

For the first example from Section 3, the algorithm works as follows:

**iteration 0** \(\rightarrow\) \(\{z^*, x - x^*, y - y^*, z - z^*\}\)

This states that \(x, y, z\) start with some unknown values \(x^*, y^*, z^*\) respectively, except that \(z\) is initialized to be 0. That is why \(z^* = 0\).

**iteration 1** \(\rightarrow\) \(\{z^*, x z - z - z x^*, -x^* y^* + z + x y, y z + z y x^* - z x^* y^* + z\}\)

**iteration 2** \(\rightarrow\) \(\{z^*, -x^* y^* + z + x y\}\)

**iteration 3** \(\rightarrow\) \(\{z^*, -x^* y^* + z + x y\}\)

Thus, in only 3 iterations, the algorithm terminates. The polynomial equation \(z^* = 0\) is the equation satisfied by the initial values. Substituting \(x^*\) and \(y^*\) in \(-x^* y^* + z + x y\) by their initial values \(X, Y\), we get the invariant \(-XY + z + x y = 0\), i.e. \(z + x y = XY\).

Let us take another example. Consider the following loop, which is an abstraction of a program in [Knu69] to find a factor of a number \(N\) with only addition and subtraction:

\[
\langle r, x, y\rangle:=\langle R^2 - N, 2R + 1, 1\rangle;
\]

**while true do**

**if true** \(\rightarrow\) \(\langle r, x, y\rangle:=(r - y, x, y + 2)\);

**[] true** \(\rightarrow\) \(\langle r, x, y\rangle:=(r + x, x + 2, y)\);

**end if**

**end while**

In this case:

\[
f_1(r, x, y) = (r - y, x, y + 2)
\]

\[
f_2(r, x, y) = (r + x, x + 2, y)
\]

\[
f_1'(r, x, y) = (r - sy - (s - 1)s, x, 2s + y)
\]

\[
f_2'(r, x, y) = (r + sx + (s - 1)s, 2s + x, y)
\]

Therefore, we just have to add one new variable \(s\):

\[
F_1(s, r, x, y) = f_1'(r, x, y) = (r - sy - (s - 1)s, x, 2s + y)
\]

\[
F_2(s, r, x, y) = f_2'(r, x, y) = (r + sx + (s - 1)s, 2s + x, y)
\]
Using \( S_0 = \{ y - 1 \} \), we get the following trace:

**iteration 0** \( \longrightarrow \{ y^* - 1, r - r^*, x - x^*, y - y^* \} \)

**iteration 1** \( \longrightarrow \{ y^* - 1, x y - y x^* - x + x^*, x^2 - (x^*)^2 - y^2 - 4 r + 4 r^* - 2 x + 2 x^* + 2 y - 1, y^3 + 4 r y - 4 y r^* - 3 y^2 - 4 r + 4 r^* + 3 y - 1 \} \)

**iteration 2** \( \longrightarrow \{ y^* - 1, x^2 - (x^*)^2 - y^2 - 4 r + 4 r^* - 2 x + 2 x^* + 2 y - 1 \} \)

**iteration 3** \( \longrightarrow \{ y^* - 1, x^2 - (x^*)^2 - y^2 - 4 r + 4 r^* - 2 x + 2 x^* + 2 y - 1 \} \)

So the algorithm terminates in 3 iterations as well. Substituting \( r^* \) and \( x^* \) by their initial values in the program \( R^2 - N \) and \( 2R + 1 \) respectively, we get that

\[-4 r - 4 N + x^2 - 2 x - y^2 + 2 y = 0\]

is invariant.

### 7 Termination of the procedure for positive eigenvalues

In this section, we give the proof of termination of the procedure provided the assignment mappings are solvable and have positive eigenvalues. For the sake of simplicity we will work in the real field \( \mathbb{R} \), and all the results will apply to the particular case of \( \mathbb{Q} \). As in Sections 5.2 and 5.1, we denote by \( \mathfrak{S}_N \) be the ideal stored in the variable \( I \) of the procedure at the end of the \( N \)-th iteration.

As a motivating example, consider the following loop:

```
\langle x, y\rangle := (0, 0);
var x, y: real end var
while true do
    if true \rightarrow \langle x, y \rangle := (x + 1, y);
        \[ true \rightarrow \langle x, y \rangle := (x, y + 1); \]
    end if
end while
```

This toy program begins with the point \((0, 0)\) and then repeatedly chooses non-deterministically to move horizontally or vertically, thus covering all the pairs of natural numbers \( \mathbb{N} \times \mathbb{N} \).

Let us apply the procedure. In this case we have that

\[
\begin{align*}
    f_1(x, y) &= (x + 1, y), & f_1^r(x, y) &= (x + s, y), & f_1^{-s}(x, y) &= (x - s, y) \\
    f_2(x, y) &= (x, y + 1), & f_2^s(x, y) &= (x, y + s), & f_2^{-s}(x, y) &= (x, y - s)
\end{align*}
\]

As both \( x \) and \( y \) are initialized to 0 before entering the loop, we take \( I_0 = \langle x^*, y^* \rangle \). So have \( \mathfrak{S}_0 := \langle x^*, y^*, x - x^*, y - y^* \rangle = \langle x^*, y^*, x, y \rangle \) after simplifying the basis. Then

\[
\begin{align*}
    \text{subs}(f_1^r, \mathfrak{S}_0) &= \langle x^*, y^*, x - s, y \rangle, & \text{subs}(f_2^s, \mathfrak{S}_0) &= \langle x^*, y^*, x, y - s \rangle
\end{align*}
\]
Now we have to compute \( \bigcap_{i=0}^{\infty} \text{subs}(f_i^{-s}, \mathcal{Z}_0) \) for \( i = 1, 2 \). If we wanted to compute a finite intersection from 0 to a certain \( N \in \mathbb{N} \), then for \( i = 1 \)

\[
\bigcap_{s=0}^{N} \text{subs}(f_1^{-s}, \mathcal{Z}_0) = \bigcap_{s=0}^{N} \langle x^*, y^*, x - s, y \rangle = \langle x^*, y^*, \prod_{s=0}^{N} (x - s), y \rangle
\]

where we have used that \( \bigcap_{s=0}^{N} (x - s) = \prod_{s=0}^{N} (x - s) \); as \( (x - s) \) is the set of all polynomials multiple of \( x - s \), \( \bigcap_{s=0}^{N} (x - s) \) is the set of common multiples for all \( x - s \) for \( 0 \leq s \leq N \); since \( \prod_{s=0}^{N} (x - s) \) is the least common multiple of these polynomials, it is a generator of \( \bigcap_{s=0}^{N} (x - s) \).

Now, if \( N = \infty \) then \( \prod_{s=0}^{N} (x - s) \) is not a polynomial anymore, and so it cannot be in the intersection. Thus \( \bigcap_{s=0}^{\infty} \text{subs}(f_1^{-s}, \mathcal{Z}_0) = \langle x^*, y^*, y \rangle \). Notice that also \( \bigcap_{s=0}^{\infty} \text{subs}(f_2^{-s}, \mathcal{Z}_0) = \langle x^*, y^*, y \rangle \) using similar arguments.

Analogously, \( \bigcap_{s=0}^{\infty} \text{subs}(f_2^{-s}, \mathcal{Z}_0) = \langle x^*, y^*, x \rangle \). Finally,

\[
\mathcal{Z}_1 := \left( \bigcap_{s=0}^{\infty} \text{subs}(f_1^{-s}, \mathcal{Z}_0) \right) \cap \left( \bigcap_{s=0}^{\infty} \text{subs}(f_2^{-s}, \mathcal{Z}_0) \right) = \langle x^*, y^*, y \rangle \cap \langle x^*, y^*, x \rangle = \langle x^*, y^*, \langle y \rangle \rangle = \langle x^*, y^*, xy \rangle
\]

as \( xy \) is the least common multiple of \( x \) and \( y \).

Let us draw the corresponding variety, together with the initial point and its successive images by \( f_1 \) and \( f_2 \). Since we cannot draw the four dimensions, we project on the \( x, y \) variables.

\[ \mathcal{V}(\langle xy \rangle) \]

\[ (0,0) \]

\[ f_2^s(0,0), \; s \in \mathbb{N} \]

\[ f_1^s(0,0), \; s \in \mathbb{N} \]
Notice that the dimension of (the projection of) \( \mathcal{V}(\mathcal{Z}_0) \) is less than the dimension of (the projection of) \( \mathcal{V}(\mathcal{Z}_1) \). Moreover, both irreducible components of \( \mathcal{V}(\mathcal{Z}_1) \), the two coordinate axes, have one dimension more than \( \mathcal{V}(\mathcal{Z}_0) \), the origin.

Now let us apply another iteration of the procedure. Using a similar argument as above \( \bigcap_{s=0}^{\infty} \text{subs}(f_1^{-s}, \mathcal{Z}_1) = \bigcap_{s=0}^{\infty} \text{subs}(f_2^{-s}, \mathcal{Z}_1) = \langle x^*, y^* \rangle \). Thus

\[
\mathcal{Z}_2 = \left( \bigcap_{s=0}^{\infty} \text{subs}(f_1^{-s}, \text{Im}_1) \right) \bigcap \left( \bigcap_{s=0}^{\infty} \text{subs}(f_2^{-s}, \mathcal{Z}_1) \right) = \langle x^*, y^* \rangle
\]

Since we do not have polynomials in the \( x, y \) variables anymore, we can ensure that at the following iteration we will terminate (without any non-trivial invariant). Besides, if we look at the projection of \( \mathcal{V}(\mathcal{Z}_2) \) on the first two variables, we get the whole plane \( \mathbb{R}^2 \), which again has one dimension more than the projection of \( \mathcal{V}(\mathcal{Z}_1) \), the coordinate axes, which had dimension 1. Moreover, again \( \bigcap_{t \in \mathbb{R}} \text{subs}(f_i^{-t}, \mathcal{Z}_1) = \bigcap_{t \in \mathbb{R}} \text{subs}(f_i^{-t}, \mathcal{Z}_1) = \langle x^*, y^* \rangle \) for \( i = 1, 2 \).

This example suggests that the dimension of the variety of the computed ideal increases at each step until termination. This is not exactly true as we will see, but the core of the proof of termination is based on this idea. What actually happens is that, at each step, either the invariant ideal has been computed, or the minimum dimension of the non-invariant irreducible components of the variety increases.

Thus, it seems convenient to study the varieties of the ideals generated by the procedure. In order to move comfortably from the language of polynomials and ideals to the language of points and varieties, we need that \( I = \Pi \mathcal{V}(I) \) be invariant in the procedure; in Section 7.2 we will see that this is the case indeed.

For both iterations in the example, we have noticed that \( \bigcap_{t \in \mathbb{R}} \text{subs}(f_i^{-t}, \mathcal{Z}_1) = \bigcap_{t \in \mathbb{R}} \text{subs}(f_i^{-t}, \mathcal{Z}_1) \) for \( i = 1, 2 \). This equality allows us to move from the discrete world of the natural numbers \( \mathbb{N} \) to the continuous world of the real numbers \( \mathbb{R} \), where dimension makes sense. In Section 7.3 we give conditions for this formula to hold.

Furthermore, in the first iteration of the example we have also seen that, although \( \mathcal{V}(\mathcal{Z}_0) \) was irreducible, \( \mathcal{V}(\mathcal{Z}_1) \) was not so. On the other hand, each mapping \( f_2 \) has led to an irreducible component in \( \mathcal{V}(\mathcal{Z}_1) \); \( f_1 \) has given the \( x \)-axis, while \( f_2 \) has given the \( y \)-axis. In Section 7.4 we study the relationship between irreducible varieties and the procedure.

Finally, Section 7.5 focuses on the conditions under which the dimension increases, and Section 7.6 gives the final proof of termination using all the previous results.

### 7.1 Basic Results

First of all, we need the following basic results from algebraic geometry on the concept of variety and annihilator, which are stated without proof:

**Lemma 4.** If \( R, S \subseteq \mathbb{R}[\hat{z}] \), then \( R \subseteq S \Rightarrow \mathcal{V}(R) \supseteq \mathcal{V}(S) \).
Lemma 5. If $A, B \subseteq \mathbb{R}^l$, then $A \subseteq B \Rightarrow \mathbb{I}(A) \supseteq \mathbb{I}(B)$.

Lemma 6. If $A \subseteq \mathbb{R}^l$, then $\mathbb{I}(A) = \bigvee \mathbb{I}(A)$.

Lemma 7. If $J, K \subseteq \mathbb{R}[z]$ are ideals, then $\bigvee(J \cap K) = \bigvee(J) \cap \bigvee(K)$.

Lemma 8. If $J, K \subseteq \mathbb{R}[z]$ are ideals, then $\mathbb{I}(\bigvee(J) \cap \bigvee(K)) = \bigvee(\mathbb{I}(J) \cap \mathbb{I}(K))$.

Now we present a couple of definitions that will make the treatment of the $\tilde{x}$ and the $\tilde{x}^*$ variables uniform.

Definition 4. For a given polynomial mapping $f \in \mathbb{R}[\tilde{x}]^m$, we define $\tilde{f} \in \mathbb{R}[\tilde{x}, \tilde{x}^*]^m$ as $\tilde{f}(\tilde{x}, \tilde{x}^*) := (f(\tilde{x}), \tilde{x}^*)$, i.e., $\tilde{f} := f \times id$.

Notice that if $f$ is solvable (affine), then $\tilde{f}$ is also a solvable (affine) mapping, and also that if $f$ is invertible then $\tilde{f}$ is invertible too.

Definition 5. Given an invertible polynomial mapping $g \in \mathbb{R}[\tilde{x}]^l$ and an ideal $J \subseteq \mathbb{R}[\tilde{z}]$, we define

$$\tilde{\text{subs}}(g, J) = \{q(g(z)) \mid q \in J\}$$

It is clear that $\tilde{\text{subs}}(g, J) \subseteq \mathbb{R}[\tilde{z}]$ is also an ideal.

The following result links the previous definitions with the operator $\text{subs}$ that we have been working with so far:

Lemma 9. Given an invertible polynomial mapping $f \in \mathbb{R}[\tilde{x}]^m$ and an ideal $I \subseteq \mathbb{R}[\tilde{x}, \tilde{x}^*]$, $\tilde{\text{subs}}(\tilde{f}, I) = \text{subs}(f, I)$.

Proof. $p \in \tilde{\text{subs}}(\tilde{f}, I) \iff \exists q \in I$ such that $p(\tilde{x}, \tilde{x}^*) = q(f(\tilde{x}), \tilde{x}^*) \iff \exists q \in I$ such that $p(\tilde{x}, \tilde{x}^*) = q(f(\tilde{x}), \tilde{x}^*) \iff p \in \text{subs}(f, I)$.

The next lemma shows the dual relation between the operator $\tilde{\text{subs}}$ and the concept of variety of an ideal.

Lemma 10. Given an invertible polynomial mapping $g \in \mathbb{R}[\tilde{x}]^l$ and an ideal $J \subseteq \mathbb{R}[\tilde{z}]$, $\bigvee(\tilde{\text{subs}}(g, J)) = g^{-1}(\bigvee(J))$.

Proof. Let us see the $\subseteq$ inclusion. Let $\tilde{\alpha} \in \bigvee(\tilde{\text{subs}}(g, J))$, and take any $p \in J$. Then $p(g(\tilde{\alpha})) = 0$ since $p \circ g \in \text{subs}(g, J)$. So $g(\tilde{\alpha}) \in \bigvee(J)$, and thus $\tilde{\alpha} \in g^{-1}(\bigvee(J))$.

For the other inclusion, let $\tilde{\alpha} \in g^{-1}(\bigvee(J))$. Then $g(\tilde{\alpha}) \in \bigvee(J)$. Now let us take any $p \in \tilde{\text{subs}}(g, J)$. Then there exists $q \in J$ such that $p = q \circ g$, and $p(\tilde{\alpha}) = q(g(\tilde{\alpha})) = 0$ since $g(\tilde{\alpha}) \in \bigvee(J)$ and $q \in J$. Therefore $\tilde{\alpha} \in \bigvee(\text{subs}(g, J))$. ∀
7.2 \( I = \mathbb{V}(I) \) Is Invariant in the Procedure

The following results are aimed at proving that \( I = \mathbb{V}(I) \) is invariant in the procedure. An ideal \( J \subseteq \mathbb{R}[\mathbb{S}] \) is such that \( J = \mathbb{V}(J) \) if and only if given \( p \in \mathbb{R}[\mathbb{S}] \):

\[
p(\tilde{\alpha}) = 0 \quad \forall \tilde{\alpha} \in \mathbb{V}(J) \iff p \in J
\]

Notice that while the \( \iff \) implication always holds, the \( \Rightarrow \) needs not to be true. If we take \( J = \langle z^2 \rangle \in \mathbb{R}[\mathbb{S}] \) we have \( \mathbb{V}(J) = \{0\} \). Then the polynomial \( p(z) = z \) satisfies \( p(0) = 0 \) but \( p \notin \langle z^2 \rangle \).

In order to prove that \( I = \mathbb{V}(I) \) is an invariant of the procedure, we have to show that it holds at the beginning, and that it is preserved at each step of the procedure; for that, we will see that the property is closed under intersection of ideals and under the mapping between ideals \( I \mapsto \bigcap_{i=0}^{\infty} \text{subs}(f^{-i}, I) \), or equivalently by \( I \mapsto \bigcap_{i=0}^{\infty} \text{subs}(f^{-i}, I) \).

First of all, the next lemma will allow us to prove that \( I = \mathbb{V}(I) \) is satisfied at the beginning of the procedure:

**Lemma 11.** If \( I_0 \subseteq \mathbb{R}[\mathbb{S}] \) is an ideal such that \( I_0 = \mathbb{V}(I_0) \) then

\[
\left( \bigcup_{j=1}^{m} \{ x_j - x_j^* \} \right) \cup I_0 = \mathbb{V} \left( \left( \bigcup_{j=1}^{m} \{ x_j - x_j^* \} \right) \cup I_0 \right)
\]

**Proof.** It is enough to show the \( \supseteq \) inclusion. Let \( p \in \mathbb{V} \left( \left( \bigcup_{j=1}^{m} \{ x_j - x_j^* \} \right) \cup I_0 \right) \). Let us consider the set \( H = \{ x_1 - x_1^*, \ldots, x_m - x_m^* \} \). Applying the division algorithm for multivariate polynomials to \( p \) and \( H \), we get certain polynomials \( r, p_j \) \((1 \leq j \leq m)\) such that

\[
p(\tilde{x}, \tilde{x}^*) = r(\tilde{x}^*) + \sum_{j=1}^{m} p_j(\tilde{x}, \tilde{x}^*)(x_j - x_j^*)
\]

Since the leading monomial of \( x_j - x_j^* \) is \( x_j \), we can guarantee that \( r \) does not depend on \( \tilde{x} \).

Now let us take \( \tilde{\alpha} \in \mathbb{V}(I_0) \). Then \((\tilde{\alpha}, \tilde{\alpha}^*) \in \mathbb{V} \left( \left( \bigcup_{j=1}^{m} \{ x_j - x_j^* \} \right) \cup I_0 \right) \), since for \( 1 \leq j \leq m \) we have

\[
(x_j - x_j^*)|_{x_j = \tilde{\alpha}^*, x_j = \tilde{\alpha}^*} = \tilde{\alpha}^*_j - \tilde{\alpha}^*_j = 0
\]

As \( p \in \mathbb{V} \left( \left( \bigcup_{j=1}^{m} \{ x_j - x_j^* \} \cup I_0 \right) \right) \),

\[
0 = p(\tilde{\alpha}, \tilde{\alpha}^*) = r(\tilde{\alpha}^*) + \sum_{i=1}^{m} p_i(\tilde{\alpha}, \tilde{\alpha}^*)(\tilde{\alpha}^*_i - \tilde{\alpha}^*_i) = r(\tilde{\alpha})
\]

Thus \( \forall \tilde{\alpha} \in \mathbb{V}(I_0) \) we have \( r(\tilde{\alpha}) = 0 \). So \( r \in \mathbb{V}(I_0) = I_0 \), and \( p \in \left( \bigcup_{j=1}^{m} \{ x_j - x_j^* \} \cup I_0 \right) \).

\( \square \)
The next lemma shows that the property \( J = \mathbb{V}(J) \) is closed under intersection:

**Lemma 12.** If \( J, K \subseteq \mathbb{R}[\mathbb{Z}] \) are ideals such that \( J = \mathbb{V}(J) \) and \( K = \mathbb{V}(K) \), then \( J \cap K = \mathbb{V}(J \cap K) \).

**Proof.** By Lemmata 7 and 8, we have that \( \mathbb{V}(J \cap K) = \mathbb{V}(J) \cap \mathbb{V}(K) = \mathbb{V}(J) \cap \mathbb{V}(K) = J \cap K \).

The goal of the following three results is to prove that the property \( J = \mathbb{V}(J) \) is preserved by \( J \mapsto \bigcap_{i=0}^{\infty} \text{subs}(g^{-i}, J) \). In order to do so, we first need to show that \( J = \mathbb{V}(J) \) is closed under the \text{subs} operator:

**Lemma 13.** If \( J \subseteq \mathbb{R}[\mathbb{Z}] \) is an ideal such that \( J = \mathbb{V}(J) \) and \( g \in \mathbb{R}[\mathbb{Z}] \) is an invertible polynomial mapping, then \( \text{subs}(g, J) = \mathbb{V}(\text{subs}(g, J)) \).

**Proof.** It is enough to show that \( \text{subs}(g, J) \supseteq \mathbb{V}(\text{subs}(g, J)) \), since the other inclusion is trivial. Let \( p \in \mathbb{V}(\text{subs}(g, J)) \). We have that \( p \in \mathbb{V}(g^{-1}(\mathbb{V}(J))) \) by Lemma 10. Now let us show that \( p \circ g^{-1} \in \mathbb{V}(J) \). Indeed, given any \( \tilde{\alpha} \in \mathbb{V}(J) \) we have \( p \circ g^{-1}(\tilde{\alpha}) = 0 \) since \( p \in \mathbb{V}(g^{-1}(\mathbb{V}(J))) \). But then \( p \circ g^{-1} \in \mathbb{V}(J) = J \), which implies that \( p = (p \circ g^{-1}) \circ g \in \text{subs}(g, J) \).

**Lemma 14.** If \( J \subseteq \mathbb{R}[\mathbb{Z}] \) is an ideal such that \( J = \mathbb{V}(J) \) and \( g \in \mathbb{R}[\mathbb{Z}] \) is an invertible polynomial mapping, then

\[
\bigcap_{i=0}^{\infty} \text{subs}(g^{-i}, J) = \mathbb{V} \left( \bigcup_{i=0}^{\infty} \mathbb{V}(\text{subs}(g^{-i}, J)) \right)
\]

**Proof.** Let us see the \( \supseteq \) inclusion. Let \( p \in \mathbb{V}(\bigcup_{i=0}^{\infty} \mathbb{V}(\text{subs}(g^{-i}, J))) \). Let us assume that \( p \notin \bigcap_{i=0}^{\infty} \text{subs}(g^{-i}, J) \) and we will get a contradiction. Under this hypothesis there exists \( s_0 \in \mathbb{N} \) such that \( p \notin \text{subs}(g^{-s_0}, J) \). Since \( p \in \bigcup_{i=0}^{\infty} \mathbb{V}(\text{subs}(g^{-s}, J)) \), in particular \( p \in \mathbb{V}(\text{subs}(g^{-s_0}, J)) = \text{subs}(g^{-s_0}, J) \) (by Lemma 13), which is impossible.

Now let us see the other inclusion. Let \( p \in \bigcap_{i=0}^{\infty} \text{subs}(g^{-i}, J) \). Then for any \( \tilde{\alpha} \in \bigcup_{i=0}^{\infty} \mathbb{V}(\text{subs}(g^{-i}, J)) \) there exists \( s_0 \in \mathbb{N} \) such that \( \tilde{\alpha} \in \mathbb{V}(\text{subs}(g^{-s_0}, J)) \). Since \( p \in \bigcap_{i=0}^{\infty} \text{subs}(g^{-i}, J) \subseteq \text{subs}(g^{-s_0}, J) \), \( p(\tilde{\alpha}) = 0 \). Therefore we have that \( p \in \mathbb{V}(\bigcup_{i=0}^{\infty} \mathbb{V}(\text{subs}(g^{-i}, J))) \).

Finally, the next proposition shows that the property \( J = \mathbb{V}(J) \) is preserved by \( J \mapsto \bigcap_{i=0}^{\infty} \text{subs}(g^{-i}, J) \):
Proposition 3. If \( J \subseteq \mathbb{R}[\mathbf{z}] \) is an ideal such that \( J = \mathbb{V}(J) \) and \( g \in \mathbb{R}[\mathbf{z}]^l \) is an invertible polynomial mapping, then
\[
\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J) = \mathbb{V}(\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J))
\]

Proof. By Lemmata 6 and 14,
\[
\mathbb{V}(\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J)) = \mathbb{V}(\bigcup_{s=0}^{\infty} \mathbb{V}(\text{subs}(g^{-s}, J))) =
\]
\[
= \mathbb{V}(\bigcup_{s=0}^{\infty} \text{subs}(g^{-s}, J)) = \bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J)
\]
\( \square \)

Finally, we have the tools to prove that \( I = \mathbb{V}(I) \) is an invariant of the procedure:

Theorem 5. If the assignment mappings \( f_i \) are invertible polynomials, then \( \forall N \in \mathbb{N} \) \( \mathbb{S}_N = \mathbb{V}(\mathbb{S}_N) \).

Proof. Let us prove it by induction over \( N \). Since \( I_0 = \mathbb{V}(I_0) \), for \( N = 0 \) we have \( \mathbb{S}_0 = \mathbb{V}(\mathbb{S}_0) \) by Lemma 11. Now let us consider the case \( N > 0 \). By induction hypothesis, we know that \( \mathbb{S}_{N-1} = \mathbb{V}(\mathbb{S}_{N-1}) \). Moreover, by Lemma 9,
\[
\mathbb{S}_N = \bigcap_{i=1}^{n} \bigcap_{s=0}^{\infty} \text{subs}(f_i^{-s}, \mathbb{S}_{N-1}) = \bigcap_{i=1}^{n} \bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathbb{S}_{N-1})
\]

By Proposition 3, for \( 1 \leq i \leq n \) we have that
\[
\bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathbb{S}_{N-1}) = \mathbb{V}(\bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathbb{S}_{N-1}))
\]
Then, by Lemma 12, \( \mathbb{S}_N = \mathbb{V}(\mathbb{S}_N) \).
\( \square \)

7.3 Intersecting over the Real Powers of Solvable Mappings

The next ingredient we need in order to prove termination is the fact that, if the assignment mappings are solvable and their eigenvalues are real and positive, then intersecting over all the natural powers is the same as intersecting over all the real powers. More precisely, if \( J \) is an ideal such that \( J = \mathbb{V}(J) \) and \( g \) is a solvable mapping with positive eigenvalues:
\[
\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J) = \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J)
\]
Example 1. For example, let $J = \{z_2\}$. Then $\forall(J) = \{(z_1, 0) \mid z_1 \in \mathbb{R}\}$, and it is easy to see that $J$ satisfies $J = \mathbb{K}(J)$. First, let us consider $g(z_1, z_2) = (z_1, z_2 + 1)$, which is a solvable mapping with a single eigenvalue 1. It is easy to see that $g'(z_1, z_2) = (z_1, z_2 + 1)$.

\[ g^2(\forall(I)) \]
\[ g(\forall(I)) \]
\[ \forall(I) \]
\[ g^{-1}(\forall(I)) \]
\[ g^{-2}(\forall(I)) \]

\[ \begin{array}{c}
\text{z}_2 \\
\text{z}_1
\end{array} \]

In order to compute $\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J)$ we use Lemmata 10 and 14 to get that

\[
\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J) = \mathbb{K} \left( \bigcup_{s=0}^{\infty} \forall(\text{subs}(g^{-s}, J)) \right) = \mathbb{K} \left( \bigcup_{s=0}^{\infty} g'(\forall(J)) \right)
\]

As regards $\bigcap_{s \in \mathbb{K}} \text{subs}(g^{-s}, J)$, extending Lemma 14 it is not difficult to see that

\[
\bigcap_{s \in \mathbb{K}} \text{subs}(g^{-s}, J) = \mathbb{K} \left( \bigcup_{s \in \mathbb{K}} g'(\forall(J)) \right)
\]

In this case we have $g'(\forall(J)) = \{(z_1, s) \mid z_1 \in \mathbb{R}\}$. Then $\bigcup_{s \in \mathbb{R}} g'(\forall(J)) = \mathbb{R}^2$, and $\bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) = \{0\}$.

On the other hand, $\bigcup_{s=0}^{\infty} g'(\forall(J)) = \mathbb{R} \times \mathbb{N}$. Then $p \in \bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J)$ if and only if $\forall \alpha \in \mathbb{R}$, $\forall \beta \in \mathbb{N} \ p(\alpha, \beta) = 0$. But since given a field $\mathbb{K}$ and $q \in \mathbb{K}^2$, $q \neq 0$ implies that $q$ has a finite number of roots, it can be proved that $\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J) = \{0\}$. So $\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J) = \bigcap_{s \in \mathbb{K}} \text{subs}(g^{-s}, J)$.

Now, let us see with another example that the above equality might not be true in general if we drop the hypotheses. For instance, if we take $g(z_1, z_2) = (-z_1, -z_2)$, which is a solvable mapping with a single eigenvalue $-1$, it can be seen that $\forall s \in \mathbb{R}$

\[
g'(z_1, z_2) = \begin{pmatrix}
\cos(s) & -\sin(s) \\
\sin(s) & \cos(s)
\end{pmatrix}
\begin{pmatrix}
z_1 \\
z_2
\end{pmatrix}
\]
that is, a counter-clockwise rotation of angle $\pi r$.

In this case $g(\mathbb{V}(J)) = \{(-z_1, 0) \mid z_1 \in \mathbb{R}\} = \mathbb{V}(J)$, and by induction, $\forall s \in \mathbb{N}$ $g^s(\mathbb{V}(J)) = \mathbb{V}(J)$, Thus, $\bigcup_{s=0}^{\infty} g^s(\mathbb{V}(J)) = \mathbb{V}(J)$ and $\bigcap_{s=0}^{\infty} \text{subs}(g^{-s}, J) = \mathbb{V}(J) = J$. But $\bigcup_{s=0}^{\infty} g^s(\mathbb{V}(J)) = \mathbb{R}^2$, and $\bigcup_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) = \{0\} \neq J$. So the equality does not hold in general if we drop the hypotheses.

Now, first of all we need to ensure that real powers of solvable mappings with positive eigenvalues make sense:

**Lemma 15.** Let $g \in \mathbb{R}[\bar{z}]$ be a solvable mapping with positive eigenvalues. Then $\forall s \in \mathbb{R}$ $g^s \in \mathbb{R}[\bar{z}]$ is a well defined polynomial mapping. In particular, $g$ is an invertible polynomial mapping.

**Proof.** It is easy to adapt Theorem 3 in Section 6 so that we can change the field $\mathbb{Q}$ by $\mathbb{R}$. Then we have for $s \in \mathbb{N}$ and for $1 \leq j \leq l g^s_j(\bar{z})$, the $j$-th component of $g^s(\bar{z})$, can be expressed as

$$g^s_j(\bar{z}) = \sum_{L=1}^{k_j} p_{jL}(s, \bar{z}) (\gamma_{jL})^s, \ 1 \leq j \leq m, \ s \geq 0$$

where for $1 \leq j \leq l$, $1 \leq L \leq k_j$, $p_{jL} \in \mathbb{R}[s, \bar{z}]$ and $\gamma_{jL} \in \mathbb{R}$. Moreover, the $\gamma_{jL}$ are products of the eigenvalues of $g$.

We only have to make sure that $\forall s \in \mathbb{R}$ the above expression makes sense. But since all the eigenvalues of $g$ are positive, all the $\gamma_{jL}$ are positive and therefore $g^s_j$ is well defined $\forall s \in \mathbb{R}$. Then it is clear that $\forall j : 1 \leq j \leq l$ and $\forall s \in \mathbb{R}$ $g^s_j(\bar{z})$ is well defined. In particular, for $s = -1$ we see that $g^{-1}(\bar{z})$ is a polynomial mapping, and so $g$ is invertible indeed.

Now we need the following technical lemma:

**Lemma 16.** Let $\varphi : \mathbb{R} \to \mathbb{R}$ be a function of the form $\varphi(s) = \sum_{\gamma \in \Gamma} p_{\gamma}(s) \gamma^s$ for a certain $\Gamma \subset \mathbb{R}^+$ which is finite and such that $\forall \gamma \in \Gamma$, $p_{\gamma} \in \mathbb{R}[s]$ and $p_{\gamma} \neq 0$. If $\forall n \in \mathbb{N} \varphi(n) = 0$, then $\Gamma = \emptyset$ (and therefore $\varphi \equiv 0$).

**Proof.** Let us assume that $\Gamma \neq \emptyset$ and we will get a contradiction. Let $\gamma_* = \max_{\gamma \in \Gamma} \gamma$. Then we have that $\forall \gamma \in \Gamma, \gamma \neq \gamma_*$ implies $\gamma < \gamma_*$, or equivalently $\gamma/\gamma_* < 1$.

Now,

$$\frac{\varphi(s)}{\gamma_*^s} = \sum_{\gamma \in \Gamma} p_{\gamma}(s) \left(\frac{\gamma}{\gamma_*}\right)^s = p_{\gamma_*}(s) + \sum_{\gamma \in \Gamma, \gamma \neq \gamma_*} p_{\gamma}(s) \left(\frac{\gamma}{\gamma_*}\right)^s$$

Taking limits as $s \to \infty$,

$$\lim_{s \to \infty} \frac{\varphi(s)}{\gamma_*^s} = \lim_{s \to \infty} p_{\gamma_*}(s)$$
And since \( \varphi(n) = 0 \) \( \forall n \in \mathbb{N} \) we have that \( \lim_{s \to \infty} \frac{\varphi(s)}{s} = \lim_{s \to \infty} p_{\varphi}(s) = 0 \), which implies \( p_{\varphi} = 0 \). But this is a contradiction.

\[
\]

Finally, we have that intersecting over all natural numbers is the same as intersecting over all real numbers:

**Proposition 4.** Let \( J \subseteq \mathbb{R}[\mathcal{S}] \) be an ideal such that \( J = \mathbb{I}\mathbb{V}(J) \) and \( g \in \mathbb{R}[\mathcal{S}] \) be a solvable mapping with positive eigenvalues. Then

\[
\bigcap_{s \geq 0} \text{subs}(g^{-s}, J) = \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J)
\]

**Proof.** It is obvious that \( \bigcap_{s \geq 0} \text{subs}(g^{-s}, J) \supseteq \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) \). Now let us see the other inclusion. Let \( p \in \bigcap_{s \geq 0} \text{subs}(g^{-s}, J) \). So \( p \in \mathbb{I}\mathbb{V}\left(\bigcup_{s \geq 0} \text{subs}(g^{-s}, J)\right) = \mathbb{I}\mathbb{V}(\mathbb{V}(J)) \) by Lemmata 10 and 14.

We want to see that \( p \in \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) \), or equivalently, that \( \forall s \in \mathbb{R} \) \( p \in \text{subs}(g^{-s}, J) = \mathbb{I}(\mathbb{V}(\text{subs}(g^{-s}, J))) = \mathbb{I}(\mathbb{V}(J)) \). So we have to see that \( \forall \bar{a} \in \mathbb{V}(J) \) and \( \forall s \in \mathbb{R} \) then \( (p \circ g^{s})(\bar{a}) = 0 \).

Now take any \( \bar{a} \in \mathbb{V}(J) \) and consider the function \( \varphi_{\bar{a}} : \mathbb{R} \to \mathbb{R}, \varphi_{\bar{a}}(s) = p(g^{s}(\bar{a})) \). Since by hypothesis \( p \in \mathbb{I}(\bigcup_{s \geq 0} g^{s}(\mathbb{V}(J))) \), we have that \( \forall s \in \mathbb{N} \) \( \varphi_{\bar{a}}(s) = p(g^{s}(\bar{a})) = 0 \). By Theorem 3 in Section 6, \( \varphi_{\bar{a}} \) is of the form as in Lemma 16. So we can apply it, and we get that \( \varphi_{\bar{a}} \equiv 0 \). Therefore \( \forall \bar{a} \in \mathbb{V}(J) \) and \( \forall s \in \mathbb{R} \) \( (p \circ g^{s})(\bar{a}) = 0 \), which is what we wanted.

\[
\]

### 7.4 Primality

The following two results show that primality is preserved under the mapping \( J \mapsto \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) \). More precisely, we will prove that if \( J \subseteq \mathbb{R}[\mathcal{S}] \) is a prime ideal such that \( J = \mathbb{I}\mathbb{V}(J) \) and \( g \in \mathbb{R}[\mathcal{S}] \) is a solvable mapping with positive eigenvalues, then

\[
\bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J)
\]

is also a prime ideal.

**Example 2.** For instance, consider \( J = \langle z_1 - 1, z_2 \rangle \). In this case \( \mathbb{V}(J) = \{(1, 0)\} \), and \( J \) satisfies that \( J = \mathbb{I}\mathbb{V}(J) \). Moreover, since \( \mathbb{V}(J) \) is clearly irreducible, \( J \) is prime. Now let us take \( g(z_1, z_2) = (2z_1, z_2) \), which is a solvable mapping with eigenvalues 1 and 2. It is clear that \( g^{s}(z_1, z_2) = (2^{s}z_1, z_2) \), and that \( \mathbb{V}(J) = \{(2, 0)\} \). Therefore \( \bigcup_{s \in \mathbb{R}} g^{s}(\mathbb{V}(J)) = \{(z_1, 0) \in \mathbb{R}^2 \mid z_1 > 0\} \). So \( \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) = \mathbb{I}\left(\bigcup_{s \in \mathbb{R}} g^{s}(\mathbb{V}(J))\right) = \langle z_2 \rangle \). And it is clear that \( \langle z_2 \rangle \) is a prime ideal, or equivalently that \( \mathbb{V}(\langle z_2 \rangle) \) is an irreducible variety. Notice that \( \dim \mathbb{V}(\langle z_2 \rangle) = 1 > 0 = \dim \{(1, 0)\} \).
Lemma 17. If $J \subseteq \mathbb{R}[x]$ is a prime ideal and $g \in \mathbb{R}[x]^I$ is an invertible polynomial mapping, then $\text{subs}(g, J)$ is also prime.

Proof. Let $p, q$ be such that $p \cdot q \in \text{subs}(g, J)$. We have to see that either $p \in \text{subs}(g, J)$ or $q \in \text{subs}(g, J)$. Indeed, as $J$ is prime, $p \cdot q \in \text{subs}(g, J) \Rightarrow (p \cdot q) \circ g^{-1} = p \circ g^{-1} \cdot q \circ g^{-1} \in J \Rightarrow p \circ g^{-1} \in J$ or $q \circ g^{-1} \in J \Rightarrow p \in \text{subs}(g, J)$ or $q \in \text{subs}(g, J)$.

□

Proposition 5. Let $J \subseteq \mathbb{R}[x]$ be a prime ideal such that $J = \mathbb{V}(J)$ and $g \in \mathbb{R}[x]^I$ be a solvable mapping with positive eigenvalues. Then $\bigcap_{x \in \mathbb{R}} \text{subs}(g^{-x}, J)$ is also a prime ideal.

Proof. Let $p, q$ be such that $pq \in \bigcap_{x \in \mathbb{R}} \text{subs}(g^{-x}, J)$. We have to see that either $p \in \bigcap_{x \in \mathbb{R}} \text{subs}(g^{-x}, J)$ or $q \in \bigcap_{x \in \mathbb{R}} \text{subs}(g^{-x}, J)$. But $pq \in \bigcap_{x \in \mathbb{R}} \text{subs}(g^{-x}, J)$ implies that $\forall s \in \mathbb{R} \; pq \in \text{subs}(g^{-s}, J)$; and as $\text{subs}(g^{-s}, J)$ is prime by Lemma 17, we have that either $p \in \text{subs}(g^{-s}, J)$ or $q \in \text{subs}(g^{-s}, J)$. Since $J = \mathbb{V}(J)$, we have $p \in \text{subs}(g^{-s}, J) \Leftrightarrow p \in \mathbb{V}(\text{subs}(g^{-s}, J)) \Leftrightarrow \forall \alpha \in \mathbb{V}(\text{subs}(g^{-s}, J)) = g^s(\mathbb{V}(J)), \; p(\alpha) = 0 \Leftrightarrow \forall \alpha \in \mathbb{V}(J), \; p(g^s(\alpha)) = 0$; and similarly for $q$.

Now let us distinguish two cases. Let us first assume that $\exists s^* \in \mathbb{R}$ such that $\forall n \in \mathbb{N} \exists s_n^* \text{ such that } |s^* - s_n^*| < 1/(n + 1)$ and $p \in \text{subs}(g^{-s^*}, J)$. Let us take an arbitrary $\alpha \in \mathbb{V}(J)$ and define the function $\varphi_\alpha : \mathbb{R} \to \mathbb{R}, \; \varphi_\alpha(s) = p(g^s(\alpha))$.

Clearly $\varphi_\alpha$ is analytical. But since $\forall n \in \mathbb{N}$ we have that $p \in \text{subs}(g^{-s^*}, J)$, then $\forall n \in \mathbb{N} \; p(g^{s_n^*}(\alpha)) = 0$; and moreover, $s_n^* \to s^*$. As $\varphi_\alpha$ is analytical, $\varphi_\alpha(s) = 0$ $\forall s \in \mathbb{R}$. Since $\alpha \in \mathbb{V}(J)$ is arbitrary, we have that $\forall \alpha \in \mathbb{V}(J) \forall s \in \mathbb{R} \; p(g^s(\alpha)) = \varphi_\alpha(s) = 0$. This implies that $\forall s \in \mathbb{R} \; p \in \text{subs}(g^{-s}, J)$, or equivalently $p \in \bigcap_{x \in \mathbb{R}} \text{subs}(g^{-x}, J)$.

Now let us assume the contrary. So let us assume that $\forall s^* \in \mathbb{R} \exists n \in \mathbb{N}$ such that $\forall s \in (s^* - 1/(n^* + 1), s^* + 1/(n^* + 1))$, then $p \notin \text{subs}(g^{-s^*}, J)$; but this implies that $q \in \text{subs}(g^{-s^*}, J)$. Let us take any $s^* \in \mathbb{R}$. Given $\alpha \in \mathbb{V}(J)$ we define the analytical function $\psi_\alpha : \mathbb{R} \to \mathbb{R}, \; \psi_\alpha(s) = q(g^s(\alpha))$. Then there exists $n^* \in \mathbb{N}$ such that $\forall s \in (s^* - 1/(n^* + 1), s^* + 1/(n^* + 1)), \; q(g^s(\alpha)) = \psi_\alpha(s) = 0$.

Thus, since $\psi_\alpha$ is analytical, $\psi_\alpha(s) = 0 \forall s \in \mathbb{R}$. Following a similar argument as above, we get that $q \in \bigcap_{x \in \mathbb{R}} \text{subs}(g^{-s}, J)$ in this case. □
7.5 Studying the Dimension of the Ideal

The next two lemmas are technical results to prove that, roughly speaking, at each step of the procedure either we have obtained the invariant ideal, or the dimension of the computed ideal increases.

Lemma 18. Let $J \subseteq \mathbb{R}[z]$ be an ideal and $g \in \mathbb{R}[z]^I$ be a solvable mapping with positive eigenvalues. Let $\tilde{\beta} \in \nabla(J)$ be such that $g(\tilde{\beta}) \notin \nabla(J)$. Then there exists $\epsilon(\tilde{\beta}) > 0$ such that $\forall \epsilon : \epsilon(\tilde{\beta}) > \epsilon > 0 : g^\epsilon(\tilde{\beta}) \notin \nabla(J)$.

Example 3. Before giving the proof, let us see an example. Let us take $J = \langle z_1 - z_2 \rangle$. In this case $\nabla(J) = \{(z, z) \in \mathbb{R}^2 \}$. Let us take $g(z_1, z_2) = (z_1 + 1, z_1 + z_2)$, which is a solvable mapping with a single eigenvalue 1. We observe that $(0, 0) \in \nabla(J)$ and $g(0, 0) = (1, 0) \notin \nabla(J)$. Moreover, $\forall s \in \mathbb{R} \; g^s(0, 0) = (s, s(s - 1)/2)$. Let us see if there is any $s \in \mathbb{R}$, $s \neq 0$ such that $g^s(0, 0) \in \nabla(J)$. We have to solve the equation

$$s = \frac{s(s - 1)}{2}$$

which has solutions $s = 0$ and $s = 3$. We are only interested in the solution $s = 3$, for which $g^3(0, 0) = (3, 3)$. Then it is clear from the graph that $\epsilon(0, 0) = 3$ is the maximal $\epsilon^*$ such that $\forall \epsilon : \epsilon^* > \epsilon > 0 : g^\epsilon(0, 0) \notin \nabla(J)$.

\begin{center}
\begin{tikzpicture}
    % Diagram code here
\end{tikzpicture}
\end{center}

Proof. Let us assume the contrary and we will get a contradiction. So let us assume that $\forall n \in \mathbb{N} \; \exists \epsilon_n$ such that $1/(n + 1) > \epsilon_n > 0$ and $g^{\epsilon_n}(\tilde{\beta}) \in \nabla(J)$.

Since $g(\tilde{\beta}) \notin \nabla(J)$, $\exists p \in J$ such that $p(g(\tilde{\beta})) \neq 0$. On the other hand, since $\forall n \in \mathbb{N} \; g^{\epsilon_n}(\tilde{\beta}) \in \nabla(J)$, $p(g^{\epsilon_n}(\tilde{\beta})) = 0$.

Now let us consider the function $\varphi : \mathbb{R} \to \mathbb{R}$, $\varphi(s) = p(g^s(\tilde{\beta}))$. Since $g$ is a solvable mapping with positive eigenvalues and $p$ is a polynomial, $\varphi$ is an analytical function. Moreover, $\forall n \in \mathbb{N} \; \varphi(\epsilon_n) = p(g^{\epsilon_n}(\tilde{\beta})) = 0$ and $\epsilon_n \to 0$. Then it must be $\varphi \equiv 0$, which is a contradiction with $\varphi(1) = p(g(\tilde{\beta})) \neq 0$.

$\Box$
Lemma 19. Let $J \subseteq \mathbb{R}[\xi]$ be an ideal and $g \in \mathbb{R}[\xi]^I$ be a solvable mapping with positive eigenvalues. Let $U$ be a non-empty open subset of $\mathbb{V}(J)$ such that $\forall \tilde{\beta} \in U$, $g(\tilde{\beta}) \notin \mathbb{V}(J)$. Then there exist $\epsilon^* > 0$ and $W \subseteq U$ non-empty open subset of $\mathbb{V}(J)$ such that $\forall \tilde{\beta} \in W$ and $\forall \epsilon : \epsilon^* > \epsilon > 0$ then $g^*(\tilde{\beta}) \notin \mathbb{V}(J)$.

Example 4. Before showing the proof, let us consider an example. Again let $J = \langle z_1 - z_2 \rangle$. Now let us take $g(z_1, z_2) = (z_1 + 1, z_2 - 1)$, which is a solvable mapping with a single eigenvalue 1. Now if $(\zeta, \zeta) \in \mathbb{V}(J) = \{(z, z) \in \mathbb{R}^2\}$ we have $g(\zeta, \zeta) = (\zeta + 1, \zeta - 1)$, and $\zeta + 1 \neq \zeta - 1 \forall \zeta \in \mathbb{R}$. So $\forall (\zeta, \zeta) \in \mathbb{V}(J), g(\zeta, \zeta) \notin \mathbb{V}(J)$. So in this case we could take $U = \mathbb{V}(J)$. Let us see now that there exist $\epsilon^* > 0$ and $W \subseteq \mathbb{V}(J)$ non-empty and open in $\mathbb{V}(J)$ such that $\forall (\zeta, \zeta) \in W \forall \epsilon : \epsilon^* > \epsilon > 0$, $g^*(\zeta, \zeta) \notin \mathbb{V}(J)$. Indeed, $\forall s \in \mathbb{R}, g^*(\zeta, \zeta) = (\zeta + s, \zeta - s)$ and $\zeta + s = \zeta - s \Leftrightarrow s = 0$. Therefore $\forall (\zeta, \zeta) \in \mathbb{V}(J) \forall s > 0, g^*(\zeta, \zeta) \notin \mathbb{V}(J)$. Therefore we can take any $\epsilon^* > 0$ and $W = \mathbb{V}(J)$.

\[
\begin{align*}
\exists \tilde{\beta} \in U \text{ such that } \forall p \in J, \forall j > 0 \text{ then } \frac{d^j}{ds^j}(p(g^*(\tilde{\beta})))|_{s=0} = 0
\end{align*}
\]

and we will get a contradiction.

Since $g(\tilde{\beta}) \notin \mathbb{V}(J)$, $\exists q \in J$ such that $q(g(\tilde{\beta})) \neq 0$. Now let us consider the analytical function $\varphi : \mathbb{R} \rightarrow \mathbb{R}, \varphi(s) = q(g^*(\tilde{\beta}))$. By hypothesis $\frac{d}{ds}\varphi(s)|_{s=0} = \frac{d}{ds}(q(g^*(\tilde{\beta})))|_{s=0} = 0 \forall j > 0$. And as $\tilde{\beta} \in \mathbb{V}(J)$, we have $\varphi(0) = q(\tilde{\beta}) = 0$. So $\frac{d}{ds}\varphi(s)|_{s=0} = 0 \forall j > 0$. Since $\varphi$ is analytical, $\varphi(0) = 0$. But this is a contradiction with $\varphi(1) = q(g(\tilde{\beta})) \neq 0$. Therefore, the following must hold:

$$\forall \tilde{\beta} \in U \exists p \in J \exists j > 0 \text{ such that } \frac{d^j}{ds^j}(p(g^*(\tilde{\beta})))|_{s=0} \neq 0$$

Now let us define

$$j^* = \min\{j \mid j > 0 \land \exists \tilde{\beta} \in U \exists p \in J \text{ such that } \frac{d^j}{ds^j}(p(g^*(\tilde{\beta})))|_{s=0} \neq 0\}$$
Let $\tilde{\beta}^* \in U$, $q \in J$ such that $\frac{d^{j^*}}{ds^{j^*}}(q(g'(\tilde{\beta}^*)))|_{s=0} \neq 0$. Then

$$\forall \tilde{\beta} \in U \forall p \in J \forall j : 0 < j < j^* \quad \frac{d^j}{ds^j}(p(g'(\tilde{\beta})))|_{s=0} = 0$$

Since $U \subseteq \forall (J)$, we have in fact that

$$\forall \tilde{\beta} \in U \forall p \in J \forall j : 0 \leq j < j^* \quad \frac{d^j}{ds^j}(p(g'(\tilde{\beta})))|_{s=0} = 0$$

In particular,

$$\forall \tilde{\beta} \in U \forall j : 0 \leq j < j^* \quad \frac{d^j}{ds^j}(q(g'(\tilde{\beta})))|_{s=0} = 0$$

Before continuing, we need to divert from the main thread of the proof. Let $(\tilde{\beta}_n) \subseteq U$ be a sequence such that $\tilde{\beta}_n \to \tilde{\beta}^*$ as $n \to \infty$. Also let us assume that, for a certain $j$ with $0 \leq j < j^*$, we have a sequence $(s_n^{(j)}) \subseteq \mathbb{R}$ such that:

i) $s_n^{(j)} > 0 \forall n \in \mathbb{N}$

ii) $s_n^{(j)} \to 0$ as $n \to \infty$

iii) $\frac{d^{j+1}}{ds^{j+1}}(q(g'(\tilde{\beta}_n)))|_{s=s_n^{(j)}} = 0 \forall n \in \mathbb{N}$

Now we are going to show how we can construct a sequence $(s_n^{(j+1)}) \subseteq \mathbb{R}$ satisfying analogous properties:

i) $s_n^{(j+1)} > 0 \forall n \in \mathbb{N}$

ii) $s_n^{(j+1)} \to 0$ as $n \to \infty$

iii) $\frac{d^{j+1}}{ds^{j+1}}(q(g'(\tilde{\beta}_n)))|_{s=s_n^{(j+1)}} = 0 \forall n \in \mathbb{N}$

Let us consider the function $\psi_{j,n} : \mathbb{R} \to \mathbb{R}$, $\psi_{j,n}(s) = \frac{d}{ds}(q(g'(\tilde{\beta}_n)))$. It is clear that $\psi_{j,n}$ is continuous and derivable in all $\mathbb{R}$, that $\psi_{j,n}(s_n^{(j)}) = 0$ by definition of $(s_n^{(j)})$ and that $\psi_{j,n}(0) = 0$ since $j < j^*$. Then, by Rolle’s theorem, $\forall n \in \mathbb{N}$ $\exists s_n^{(j+1)} \in (0, s_n^{(j)})$ such that

$$\frac{d}{ds}(\psi_{j,n}(s))|_{s=s_n^{(j+1)}} = \frac{d^{j+1}}{ds^{j+1}}(q(g'(\tilde{\beta}_n)))|_{s=s_n^{(j+1)}} = 0$$

Clearly the sequence $(s_n^{(j+1)})$ also satisfies $\forall n \in \mathbb{N}$ $s_n^{(j+1)} > 0$ and $s_n^{(j+1)} \to 0$ as $n \to \infty$.

Finally, let us recover the thread of the proof and show that $\exists \epsilon* > 0 \exists \epsilon > 0$ such that $\forall \tilde{\beta} \in U$ with $||\tilde{\beta} - \tilde{\beta}^*|| < \epsilon$ and $\forall \epsilon : \epsilon > \epsilon > 0$, $g'(\tilde{\beta}) \notin \forall (J)$. Let us assume the contrary and we will get a contradiction. In this case, we can construct a sequence $(\tilde{\beta}_n) \subseteq U$ such that $\tilde{\beta}_n \to \tilde{\beta}^*$ and a sequence $(\epsilon_n) \subseteq \mathbb{R}$ such that $\epsilon_n > 0 \forall n \in \mathbb{N}$, $\epsilon_n \to 0$ and $g'(\tilde{\beta}_n) \notin \forall (J)$; in particular, $q(g'(\tilde{\beta}_n))|_{s=\epsilon_n} = 0$. Applying repeatedly the above scheme, we obtain a sequence $(\epsilon_n') \subseteq \mathbb{R}$ such that $\epsilon_n' > 0 \forall n \in \mathbb{N}$, $\epsilon_n' \to 0$ and $\frac{d^{j+1}}{ds^{j+1}}(q(g'(\tilde{\beta}_n)))|_{s=\epsilon_n'} = 0$. Now, the function $\phi : \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}$, $\phi(x,t) = \frac{d^{j+1}}{ds^{j+1}}(q(g'(x)))|_{s=\epsilon}$ is continuous. Since $\phi(\tilde{\beta}_n, \epsilon_n') = 0$
\(\forall n \in \mathbb{N} \text{ and } \beta_n \to \beta^* \text{ and } \epsilon_n \to 0 \text{ as } n \to \infty, \text{ by continuity we get that } \frac{d^*}{dx}(g(\beta^*))|_{x=\epsilon} = \phi(\beta^*, 0) = 0, \text{ which is impossible.}\\

Therefore, \(\exists \epsilon^* > 0 \forall r > 0 \text{ such that } \forall \beta \in U \text{ with } ||\beta - \beta^*|| < r \text{ and } \forall \epsilon : \epsilon^* > \epsilon > 0, g'(\beta) \notin \mathbb{V}(J)\); now if we take \(W = \{\beta \in U | ||\beta - \beta^*|| < r\} \text{ we are done.} \)

Finally, the next proposition will provide us with the formal justification that, at each step, either the invariant ideal has been computed, or the minimum dimension of the non-invariant irreducible components of the variety of \(I\) increases.

**Proposition 6.** Let \(J \subseteq \mathbb{R}[\mathbb{E}]\) be a prime ideal such that \(J = \mathbb{F}(J)\) and \(g \in \mathbb{R}[\mathbb{E}]^I\) be a solvable mapping with positive eigenvalues such that \(g(\mathbb{F}(J)) \subseteq \mathbb{F}(J)\). Then \(\mathbb{V}(\cap_{s \in \mathbb{R}} \mathbb{F}(g^{-s}, J))\) is an irreducible variety such that

\[
\dim \mathbb{V}(\cap_{s \in \mathbb{R}} \mathbb{F}(g^{-s}, J)) > \dim \mathbb{V}(J)
\]

**Proof.** By Proposition 5, we have that \(\mathbb{V}(\cap_{s \in \mathbb{R}} \mathbb{F}(g^{-s}, J))\) is an irreducible variety.

Now let us distinguish two cases. Let us first assume that \(\dim \mathbb{V}(J) = 0\). Since \(g(\mathbb{F}(J)) \notin \mathbb{F}(J)\), there exists \(\beta \in \mathbb{F}(J)\) such that \(g(\beta) \notin \mathbb{F}(J)\). Then by Lemma 18 we know that there exists \(\delta > 0\) such that \(\forall \epsilon : \delta \geq \epsilon > 0 : g'(\beta) \notin \mathbb{F}(J)\).

Let us consider the mapping \(\varphi : [0, \delta] \to \{g'(\beta) \mid s \in [0, \delta]\}, \varphi(s) = g'(\beta)\). Clearly \(\varphi\) is continuous and surjective. Let us see that it is injective. If there exist \(s, t \in [0, \delta]\) such that \(s \geq t \text{ and } \varphi(s) = g'(\beta) = g'(\beta) = \varphi(t)\), then \(g^{-s}(-\delta) = \beta\). But this implies \(g^{-s}(-\delta) \in \mathbb{F}(J)\) and \(s - t \in [0, \delta]\). Then it must be \(s - t = 0\), and \(\varphi\) is injective indeed. Now \([0, \delta]\) is compact and \(\{g'(\beta) \mid s \in [0, \delta]\}\) is Hausdorff, with the topology induced by \(\mathbb{R}\) and \(\mathbb{R}^I\) respectively. By a well known result of topology, we have that \(\varphi\) is an homeomorphism. But

\[
\{g'(\beta) \mid s \in [0, \delta]\} \subseteq \bigcup_{s \in \mathbb{R}} g'(\mathbb{F}(J)) \subseteq \mathbb{V}(\bigcup_{s \in \mathbb{R}} g'(\mathbb{F}(J))) = \mathbb{V}\left(\bigcap_{s \in \mathbb{R}} \mathbb{F}(g^{-s}, J)\right)
\]

which implies that

\[
\dim \mathbb{V}(\cap_{s \in \mathbb{R}} \mathbb{F}(g^{-s}, J)) > \dim \mathbb{V}(J) = 0
\]

Let us consider the other case, \(\dim \mathbb{V}(J) = d > 0\). As \(g(\mathbb{F}(J)) \notin \mathbb{F}(J)\), \(\exists \beta^* \in \mathbb{F}(J)\) such that \(g'(\beta^*) \notin \mathbb{F}(J)\). Since \(\mathbb{F}(J)\) is a closed set in the topology induced by \(\mathbb{R}^I\), \(\exists S \subseteq \mathbb{R}^I\) open such that \(g(S) \in \mathbb{F}(S) \cap \mathbb{F}(J) = \emptyset\). As \(g : \mathbb{R}^I \to \mathbb{R}^I\) is a continuous mapping, \(g^{-1}(S)\) is an open subset of \(\mathbb{R}^I\). So \(U = \mathbb{F}(J) \cup g^{-1}(S)\) is an open set of \(\mathbb{F}(J)\) and \(\beta^* \in U\). Moreover, \(\forall \beta \in U, g(\beta) \notin \mathbb{F}(J)\). Then, by Lemma 19, there exist \(\delta > 0 \text{ and } W \subseteq U \text{ non-empty open subset of } \mathbb{F}(J)\) such that \(\forall \beta \in W \text{ and } \forall \epsilon : \delta \geq \epsilon > 0, g'(\beta) \notin \mathbb{F}(J)\).
It is clear that there exist a compact subset $V \subseteq W$ and an homeomorphism
\[
\phi : [0, 1]^d \rightarrow V
\]
Let us define the mapping $\varphi : [0, 1]^d \times [0, \delta] \rightarrow \bigcup_{s \in [0, \delta]} \{ g^s(V) \}$, $\varphi(u, s) = g^s(\phi(u))$. It is clear that $\varphi$ is continuous and surjective. Let us see that it is injective. If there exist $s, t \in [0, \delta]$ and $u, v \in [0, 1]^d$ such that $s \geq t$ and $\varphi(u, s) = g^s(\phi(u)) = g^t(\phi(v)) = \varphi(v, t)$, then $g^{s-t}(\phi(u)) = \phi(v)$. But this implies $g^{s-t}(\phi(u)) \in \forall(J)$ and $s - t \in [0, \delta]$. Then it must be $s - t = 0$, i.e. $s = t$. Then, since $g^s$ is invertible and $\phi$ is an homeomorphism, we have $g^s(\phi(u)) = g^s(\phi(v)) \Rightarrow \phi(u) = \phi(v) \Rightarrow u = v$. So $\varphi$ is injective. But $[0, 1]^d \times [0, \delta]$ is compact and $\bigcup_{s \in [0, \delta]} \{ g^s(V) \}$ is Hausdorff, with the topology induced by $\mathbb{R}^{d+1}$ and $\mathbb{R}^d$ respectively. Again we have that $\varphi$ is an homeomorphism. And
\[
\bigcup_{s \in [0, \delta]} \{ g^s(V) \} \subseteq \bigcup_{s \in \mathbb{R}} g^s(\forall(J)) \subseteq \forall\left( \bigcup_{s \in \mathbb{R}} g^s(\forall(J)) \right) = \forall\left( \bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J) \right)
\]
implies that
\[
\text{dim} \forall(\bigcap_{s \in \mathbb{R}} \text{subs}(g^{-s}, J)) > \text{dim} \forall(J) = d
\]
\[\square\]

7.6 Proof of Termination

Before proving the main result of this section, we still need the next technical lemma:

**Lemma 20.** If $J, K \subseteq \mathbb{R}[\mathbb{F}]$ are ideals and $g \in \mathbb{R}[\mathbb{F}]^d$ is an invertible polynomial mapping, then $\text{subs}(g, J \cap K) = \text{subs}(g, J) \cap \text{subs}(g, K)$.

**Proof.** Let us see $\subseteq$. Let $p \in \text{subs}(g, J \cap K)$. Then there exists $q \in J \cap K$ such that $p = q \circ g$. Since $q \in J$, $p \in \text{subs}(g, J)$. And as $q \in K$, $p \in \text{subs}(g, K)$. So $p \in \text{subs}(g, J) \cap \text{subs}(g, K)$.

Now let us see $\supseteq$. Let $p \in \text{subs}(g, J) \cap \text{subs}(g, K)$. Then there exist $q \in J$ such that $p = q \circ g$ and $r \in K$ such that $p = r \circ g$. Thus $q = r \circ g \circ g^{-1} = p \circ g^{-1} = r \circ g \circ g^{-1} = r$, as $g$ is invertible. So $r = q \in J \cap K$ and $p \in \text{subs}(g, J \cap K)$.

\[\square\]

We also recall the following basic result from algebraic geometry (see [CLO98] for example):

**Theorem 6.** Any variety $V$ can be uniquely expressed as a finite union of irreducible varieties $V_i$ with $V_i \notin V_j$ for $i \neq j$ (i.e. they are irredundant).

The varieties $V_i$ appearing in this unique decomposition are called the irreducible components of $V$. 
Finally we give the proof of termination of the procedure. We remind that we denote by \( \mathcal{N} \) the ideal that is stored in the variable \( I \) at the end of the \( N \)-th iteration.

The main idea is as follows. We first show that \( \forall (\mathcal{N}_{N+1}) \) can be decomposed as the union of: i) the irreducible components of \( \forall (\mathcal{N}_N) \) that are invariant, in the sense that they are preserved by all assignment mappings; and ii), other irreducible varieties related to the non-invariant irreducible components of \( \forall (\mathcal{N}_N) \). Moreover, the minimum dimension of the varieties in ii) is strictly greater than the minimum dimension of the non-invariant irreducible components of \( \forall (\mathcal{N}_N) \). But if \( \mathcal{N}_{N+1} \) is not the invariant ideal, and therefore there are irreducible components of \( \forall (\mathcal{N}_{N+1}) \) which are not invariant, then these components must appear in ii). Thus, the minimum dimension of the non-invariant irreducible components has increased. However, it is clear that this dimension cannot increase indefinitely; since we are working with the \( 2m \) variables \( x_1, \ldots, x_m, x_1', \ldots, x_m' \), we get the final bound \( 2m + 1 \).

**Theorem 7.** If the assignment mappings of the loop \( f_i \in \mathbb{R}[x]^m \) are solvable mappings with positive eigenvalues, i.e. \( \bigcup_{i=1}^{n} \text{eigenvalues}(f_i) \subseteq \mathbb{R}^+ \), then the procedure terminates in at most \( 2m + 1 \) iterations.

**Proof.** First of all, notice that by Theorem 5, \( \mathcal{N} = \forall (\mathcal{N}) \forall N \in \mathbb{N} \).

Now let \( V_1, \ldots, V_{k(N)} \) be the decomposition of \( \forall (\mathcal{N}) \) into (irreducible) irreducible varieties. We define \( \mathcal{N}^{(i)} : = \forall (V_j) \). Then we have that the \( \mathcal{N}^{(i)} \) are prime ideals, that

\[
\forall (\mathcal{N}^{(i)}) = \forall (V_j) = \mathcal{N}^{(i)}
\]

and that

\[
\mathcal{N} = \forall (\mathcal{N}) = \forall \left( \bigcup_{j=1}^{k(N)} V_j \right) = \bigcap_{j=1}^{k(N)} \forall (V_j) = \bigcap_{j=1}^{k(N)} \mathcal{N}^{(i)}
\]

Then, using the above equation and Lemma 20,

\[
\mathcal{N}_{N+1} = \bigcap_{i=1}^{n} \bigcap_{s=0}^{\infty} \text{subs}(f_i^{-s}, \mathcal{N}_N) = \bigcap_{i=1}^{n} \bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathcal{N}_N) = \bigcap_{i=1}^{n} \bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathcal{N}^{(i)}_N)
\]

and

\[
\forall (\mathcal{N}_{N+1}) = \forall \left( \bigcap_{i=1}^{n} \bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathcal{N}^{(i)}_N) \right) = \bigcup_{j=1}^{k(N)} \bigcup_{i=1}^{n} \forall \left( \bigcap_{s=0}^{\infty} \text{subs}(\tilde{f}_i^{-s}, \mathcal{N}^{(i)}_N) \right)
\]

Notice that if \( \exists i : 1 \leq i \leq n \) and \( \exists j : 1 \leq j \leq k(N) \) such that \( \tilde{f}_i(\forall (\mathcal{N}^{(j)}_N)) \subseteq \forall (\mathcal{N}^{(i)}_N) \), then by induction \( \forall s \in \mathbb{N} \tilde{f}_i(\forall (\mathcal{N}^{(j)}_N)) \subseteq \forall (\mathcal{N}^{(i)}_N) \); and therefore \( \forall s \in \mathbb{N} \mathcal{N}^{(j)}_N = \forall (\mathcal{N}^{(j)}_N) \subseteq \forall (\tilde{f}_i(\forall (\mathcal{N}^{(j)}_N))) = \forall (\text{subs}(\tilde{f}_i^{-s}, \mathcal{N}^{(j)}_N)) = \text{subs}(\tilde{f}_i^{-s}, \mathcal{N}^{(j)}_N) \).
As \( \exists_N^{(j)} = \widehat{\text{subs}}(f_i, \exists_N^{(j)}) \), from the above inclusion \( \exists_N^{(j)} = \cap_{i=0}^\infty \widehat{\text{subs}}(f_i^{s}, \exists_N^{(j)}) \) and \( \forall (\exists_N^{(j)}) = \forall (\cap_{i=0}^\infty \text{subs}(f_i^{s}, \exists_N^{(j)})) \),

So we can split the \( \exists_N^{(j)} \) according to the existence or not of such \( i \) and \( j \) as follows:

\[
\forall (\exists_{N+1}) = \bigcup_{j=1}^{k(N)} \bigcup_{i=0}^{n} \forall \left( \bigcap_{s=0}^\infty \widehat{\text{subs}}(f_i^{s}, \exists_N^{(j)}) \right)
\]

\[
= \left( \bigcup_{1 \leq i \leq n, 1 \leq j \leq k(N)} \forall \left( \bigcap_{s=0}^\infty \widehat{\text{subs}}(f_i^{s}, \exists_N^{(j)}) \right) \right)
\]

\[
= \left( \bigcup_{1 \leq i \leq n, 1 \leq j \leq k(N)} \forall \left( \bigcap_{s=0}^\infty \widehat{\text{subs}}(f_i^{s}, \exists_N^{(j)}) \right) \right)
\]

The last equality follows from the fact that if \( \exists_i, i': 1 \leq i, i' \leq n \) such that

\[
\tilde{f}_i(\forall (\exists_N^{(j)})) \subseteq \forall (\exists_N^{(j)}) \quad \text{and} \quad \tilde{f}_{i'}(\forall (\exists_N^{(j)})) \notin \forall (\exists_N^{(j)})
\]

then

\[
\forall (\exists_N^{(j)}) \subseteq \forall \left( \bigcap_{s=0}^\infty \widehat{\text{subs}}(f_i^{s}, \exists_N^{(j)}) \right)
\]

and, therefore, the points in \( \forall (\exists_N^{(j)}) \) are already taken into account on the right-hand side of the union in \( \forall (\cap_{i=0}^\infty \text{subs}(f_i^{s}, \exists_N^{(j)})) \).

By Propositions 4 and 5, all the varieties in this decomposition are irreducible. So the varieties in the (unique irredundant) irreducible decomposition of \( \forall (\exists_{N+1}) \) must appear in the above union. We will use that in the inequality (*) below.

At each step of the procedure we may have two cases. Either \( \forall i, j: 1 \leq i \leq n, 1 \leq j \leq k(N) \) \( \tilde{f}_i(\forall (\exists_N^{(j)})) \subseteq \forall (\exists_N^{(j)}) \), and so \( \exists_N^{(j)} = \cap_{i=0}^\infty \text{subs}(f_i^{s}, \exists_N^{(j)}) \) and \( \exists_N = \exists_{N+1} = \text{P} \). Or \( \exists_i, j: 1 \leq i \leq n, 1 \leq j \leq k(N) \) such that \( \tilde{f}_i(\forall (\exists_N^{(j)})) \notin \forall (\exists_N^{(j)}) \). In this case we can define

\[
\mu(\exists_N) = \min \{ \dim (\forall (J)) \mid i: 1 \leq i \leq n \text{ such that } \tilde{f}_i(\forall (J)) \notin \forall (J) \}
\]

and \( \forall (J) \) is an irreducible component of \( \forall (\exists_N) \).
It is clear that, under the hypothesis, \( \mu(\mathcal{Z}_N) \) is well defined.

Now, let us assume that the procedure takes more than \( 2m + 1 \) iterations to terminate, and we will get a contradiction. In this case we have that \( \forall N : 0 \leq N \leq 2m, \mathcal{Z}_N \neq \mathcal{Z}_{N+1} \). In particular, this implies that \( \forall N : 0 \leq N \leq 2m \exists i,j : 1 \leq i \leq n, 1 \leq j \leq k(N) \) such that \( \tilde{f}_i(\mathcal{V}(\mathcal{Z}_N^{(j)})) \nsubseteq \mathcal{V}(\mathcal{Z}_N^{(j)}) \). Therefore, \( \forall N : 0 \leq N \leq 2m \mu(\mathcal{Z}_N) \) is well defined.

Let us show that \( \forall N : 0 \leq N \leq 2m, \mu(\mathcal{Z}_N) < \mu(\mathcal{Z}_{N+1}) \). Indeed, using Propositions 4 and 6:

\[
\mu(\mathcal{Z}_{N+1}) = \min \{ \dim \mathcal{V}(J) \mid \exists i : 1 \leq i \leq n \text{ such that } \tilde{f}_i(\mathcal{V}(J)) \nsubseteq \mathcal{V}(J) \text{ and } \mathcal{V}(J) \text{ is an irreducible component of } \mathcal{V}(\mathcal{Z}_{N+1}) \} \geq \tag{*} \min \left\{ \dim \mathcal{V} \left( \bigcap_{s=0}^{\infty} \text{sub}(\tilde{f}_s^{-s}, \mathcal{Z}_N^{(j)}) \right) \bigg| 1 \leq j \leq k(N), 1 \leq i \leq n \text{ s.t. } \tilde{f}_i(\mathcal{V}(\mathcal{Z}_N^{(j)})) \nsubseteq \mathcal{V}(\mathcal{Z}_N^{(j)}) \right\} > \min \{ \dim \mathcal{V}(\mathcal{Z}_N^{(j)}) \mid 1 \leq j \leq k(N), \exists i : 1 \leq i \leq n \text{ s.t. } \tilde{f}_i(\mathcal{V}(\mathcal{Z}_N^{(j)})) \nsubseteq \mathcal{V}(\mathcal{Z}_N^{(j)}) \} = \mu(\mathcal{Z}_N) \]

As \( \mu(\mathcal{Z}_0) \geq 0 \), by induction \( \forall N : 0 \leq N \leq 2m \) we have \( \mu(\mathcal{Z}_N) \geq N \). In particular, \( \mu(\mathcal{Z}_{2m}) \geq 2m \). Therefore, \( \mathcal{V}(\mathcal{Z}_{2m}) = \mathbb{R}^{2m} \) and \( \mathbb{R}^{2m} \) is the only irreducible component of \( \mathcal{V}(\mathcal{Z}_{2m}) \). But this is a contradiction with the fact that \( \exists i : 1 \leq i \leq n \) such that \( \tilde{f}_i(\mathcal{V}(\mathcal{Z}_{2m})) \nsubseteq \mathcal{V}(\mathcal{Z}_{2m}) \).

\( \square \)

8 Examples

Below we show some of the loops whose polynomial invariants have been successfully computed using our implementation in Maple. In each case we also indicate, for each iteration, the dimension of the variety corresponding to the ideal obtained, in order to illustrate the ideas presented in Section 7.

Example 5. The following example is a program for computing the floor of the square root of a natural number:

```plaintext
function sqrt (N: integer) returns a: integer
{ Pre: N \geq 0 }  
var s, t: integer end var
(a, s, t):=(0, 1, 1);  
{ Inv: s - t \leq N }  
while s \leq N do
{ (a, s, t) :=(a + 1, s + t + 2, t + 2); 
end while
```
\{ \text{Post: } a^2 \leq N < (a+1)^2 \}\]

end function

Applying the algorithm to the abstraction of the loop, we get:

iteration 0 \rightarrow
\{t^* - 1, s^* - 1, a^*, a - a^*, s - s^*, t - t^*\}, \text{dimension 0}

iteration 1 \rightarrow
\{t^* - 1, s^* - 1, a^*, 2a - t + 1, a^2 - s + 2a + 1\}, \text{dimension 1}

iteration 2 \rightarrow
\{t^* - 1, s^* - 1, a^*, 2a - t + 1, a^2 - s + 2a + 1\}, \text{dimension 1}

So the conjunction \( t = 2a + 1 \land s = a^2 + 2a + 1 \) is automatically generated as an invariant in 2 iterations.

Example 6. The subsequent loop has been extracted from [CC77]:

\begin{verbatim}
var i, j: integer end var
\langle i, j \rangle := \langle 2, 0 \rangle;
while true do
  if true \rightarrow
    \langle i, j \rangle := \langle i + 4, j \rangle;
  \end if
  \langle i, j \rangle := \langle i + 2, j + 1 \rangle;
end while
\end{verbatim}

For this case we get the following ideals:

iteration 0 \rightarrow
\{j^*, \ i^* - 2, i - i^*, j - j^*\}, \text{dimension 0}

iteration 1 \rightarrow
\{j^*, \ i^* - 2, ji - 2j - 2j^2\}, \text{dimension 1}

iteration 2 \rightarrow
\{j^*, \ i^* - 2\}, \text{dimension 2}

iteration 3 \rightarrow
\{j^*, \ i^* - 2\}, \text{dimension 2}

After 3 iterations the algorithm stabilizes but no loop invariant is generated, as the polynomials \( j^*, i^* - 2 \) describe the initial values of the variables. Since our technique is complete, i.e., if there is a polynomial equation which is invariant in the loop, the algorithm will find the strongest conjunction of such invariant polynomial equations, it can be asserted that there are no non-trivial invariant polynomial equations in the above loop. This is consistent with the results obtained by Cousot and Halbwachs, who do not find linear invariant equalities for this example.
Example 7. The next example, taken from [Dij76], is a version of Euclid’s algorithm that computes the least common multiple of two natural numbers instead of its greatest common divisor.

**function** lcm \((a, b): \text{integer}\) **returns** \(z: \text{integer}\)

\[
\begin{align*}
&\text{Pre}: a > 0 \land b > 0 \\
&\text{var } x, y, u, v: \text{integer} \ \text{end var} \\
&(x, y, u, v) := (a, b, a); \\
&\{ \text{Inv: } \gcd(x, y) = \gcd(a, b) \} \\
&\text{while } x \neq y \text{ do} \\
&\quad \text{if } x > y \rightarrow \\
&\qquad (x, y, u, v) := (x - y, y, u, u + v); \\
&\quad \text{end if} \\
&\text{end while} \\
&z := (u + v)/2; \\
&\{ \text{Post: } z = \text{lcm}(a, b) \} \\
\end{align*}
\]

end **function**

If we apply the algorithm to the abstraction of the above program, we get:

**iteration 0** \(\rightarrow \)
\[
\{ x^* - v^*, y^* - u^*, x - x^*, y - y^*, u - u^*, v - v^* \}, \text{dimension 2}
\]

**iteration 1** \(\rightarrow \)
\[
\{ y^* - u^*, y + u - 2u^*, x^* - v^*, x + v - 2v^*, uv - uv^* - vu^* + u^*v^* \}, \text{dimension 3}
\]

**iteration 2** \(\rightarrow \)
\[
\{ y^* - u^*, x^* - v^*, ux - 2u^*v^* + vy, -2xu^* + xy + uv - 2vu^* - 2yu^* - 2u^*v^* + 6u^*v^*, 2yuv^* - 2yu^*v^* + vy^2 - u^2v + 2u^2v^* - 6u^*v^* + 2uvu^* + 4u^*v^* - 2yu^* \}, \text{dimension 4}
\]

**iteration 3** \(\rightarrow \)
\[
\{ y^* - u^*, x^* - v^*, ux - 2u^*v^* + vy \}, \text{dimension 5}
\]

**iteration 4** \(\rightarrow \)
\[
\{ y^* - u^*, x^* - v^*, ux - 2u^*v^* + vy \}, \text{dimension 5}
\]

The invariant \(ux + vy = 2ab\) is obtained after substituting by the initial values of the variables \(u^*\) and \(v^*\).

Example 8. The following program is yet another version of Euclid’s algorithm. It computes the greatest common divisor of two natural numbers together with Bezout’s coefficients:

**function** euclid_extended \((x, y): \text{integer}\) **returns** \(a, p, r: \text{integer}\)

\[
\begin{align*}
&\text{Pre}: x > 0 \land y > 0 \\
&\text{var } x, y, u, v, a, b, p, r: \text{integer} \ \text{end var} \\
&(x, y, u, v, a, b, p, r) := (x, y, u, v, a, b, p, r); \\
&\{ \text{Inv: } \gcd(x, y) = \gcd(a, b) \} \\
&\text{while } x \neq y \text{ do} \\
&\quad \text{if } x > y \rightarrow \\
&\qquad x := x - y; \\
&\quad \text{end if} \\
&\text{end while} \\
&a := x; \\
&\{ \text{Post: } a = \gcd(x, y) \} \\
\end{align*}
\]

end **function**
\textbf{var} b, q, s; \textbf{integer} end \textbf{var}
\begin{align*}
(a, b, p, q, r, s) & := \langle x, y, 1, 0, 0, 1 \rangle; \\
\{ \text{inv:} \gcd(x, y) &= \gcd(a, b) \}
\end{align*}
\begin{algorithmic}
\While{a \neq b}
\If{a > b}
\langle a, b, p, q, r, s \rangle := \langle a - b, b, p - q, q, r - s, s \rangle;
\Else
\langle a, b, p, q, r, s \rangle := \langle a - a, b, q - p, r, s - r \rangle;
\EndIf
\EndWhile
\{ Post: \gcd(x, y) = px + ry \}
\end{algorithmic}

For this program we get:

\textbf{iteration 0} \rightarrow
\{ p^* - 1, q^*, r^*, s^* - 1, a - a^*, b - b^*, p - p^*, q - q^*, r - r^*, s - s^* \}, \text{ dimension 2}

\textbf{iteration 1} \rightarrow
\{ s^* - 1, s - 1, r^*, q^*, p^* - 1, p - 1, q r - a + a^* + r b^*, b r - a + a^*, q a^* - b + b^*, q a - b + b^*, b a - b a^* - a b^* + a^* b^* \}, \text{ dimension 3}

\textbf{iteration 2} \rightarrow
\{ s^* - 1, r^*, q^*, p^* - 1, s p - s - p + 1, q r - p - s + 2, b r + a^* - s a, q a^* - b + s b^*, b p - q a - b^*, a^* p - a + r b^*, - s a + s a^* + s r b^* + a - a^* - r b^*, s q a - q a - s b + s b^* + b - b^*, s^2 b^* a - s b a + a^* s b - a s b^* - a^* s b^* + b a - b a^* + a^* b^* \}, \text{ dimension 4}

\textbf{iteration 3} \rightarrow
\{ s^* - 1, r^*, q^*, p^* - 1, - s p + 1 + q r, b r + a^* - s a, q a^* - b + s b^*, b p - q a - b^*, a^* p - a + r b^* \}, \text{ dimension 5}

\textbf{iteration 4} \rightarrow
\{ s^* - 1, r^*, q^*, p^* - 1, - s p + 1 + q r, b r + a^* - s a, q a^* - b + s b^*, b p - q a - b^*, a^* p - a + r b^* \}, \text{ dimension 5}

In this case, after substituting by the initial values, our procedure yields the conjunction:

\[ 1 + q r - s p = 0 \land r b - s a + x = 0 \land s y + q x - b = 0 \land b p - a q - y = 0 \land y r + x p - a = 0 \]

as an invariant in 4 iterations.

\textit{Example 9.} Our last loop was introduced in Section 3:
\begin{align*}
(a, b, p, q) & := \langle A, B, 1, 0 \rangle; \\
\textbf{while} \text{ true do} \\
\textbf{if} \text{ true} \rightarrow \langle a, b, p, q \rangle := \langle a - 1, b, p, q + b p \rangle; \\
\textbf{else true} \rightarrow \langle a, b, p, q \rangle := \langle a / 2, b / 2, 4 p, q \rangle;
\end{align*}
end if
end while

For this loop the trace of ideals and dimensions is:

iteration 0 $\rightarrow$
\{q^*, p^* - 1, a - a^*, b - b^*, p - p^*, q - q^*\}, dimension 2

iteration 1 $\rightarrow$
\{q^*, p^* - 1, pq - q, qb - qb^*, ba^* - b^*a - q, b^*aq - qa^*b^* + q^2, pb^2 - b^*2, bpa - a^*b^* + q, a^2p^2 - a^2b^2 - pa^*2 + a^*2, a^2pb^2 - a^2b^* + qa + qa^*\}, dimension 3

iteration 2 $\rightarrow$
\{q^*, p^* - 1, pb^2 - b^*2, bpa - a^*b^* + q, ba^*b^* - b^*a - qb, a^2pb^2 - a^2b^* + qa + qa^*\}, dimension 4

iteration 3 $\rightarrow$
\{q^*, p^* - 1, pb^2 - b^*2, bpa - a^*b^* + q, ba^*b^* - b^*a - qb, a^2pb^2 - a^2b^* + qa + qa^*\}, dimension 4

After substituting by the initial values, we get the invariant

\[ pb^2 = B^2 \land bpa + q = AB \land bAB = B^2a + qb \land a^2pB^2 + 2qAB = A^2B^2 + q^2 \]

Finally, in the examples showed in Section 6.1 we did not give the dimension for the ideals we obtained in the execution of the procedure. For both examples the trace of dimensions is \( 2 - 3 - 4 \).

9 Conclusion

The main contributions of this paper are:

1. We prove that the set of invariant polynomials of a loop has the algebraic structure of an ideal. Moreover, for any finite basis of this ideal, the corresponding conjunction of polynomial equations is the strongest possible inductive conjunction of polynomial equations for the loop. By Hilbert’s basis theorem, such a finite basis exists. Therefore, this is an existential result.
2. For assignment mappings which are solvable and commute, i.e. \( f_i \circ f_j = f_j \circ f_i \) for \( 1 \leq i, j \leq n \), we show that the invariant ideal is computed in \( n + 1 \) steps, where \( n \) is the number of branches in the body of the loop.
3. For assignment mappings which are solvable and have positive eigenvalues, we prove that the invariant ideal is computed in \( 2m + 1 \) steps, where \( m \) is the number of changing variables in the loop.
4. We explain how the procedure for computing the invariant ideal can be approximated using Gröbner bases. And moreover, for solvable mappings with rational positive eigenvalues we prove that this approximation is exact.
i.e., the algorithm computes the invariant ideal from which the strongest inductive conjunction of polynomial equations can be obtained. Furthermore, if the invariant ideal computed by the algorithm is the trivial ideal \( \{0\} \), then it can be asserted that the loop does not have any non-trivial invariant conjunction of polynomial equations.

5. The algorithm has been implemented in Maple and successfully used to compute invariant conjunctions of polynomial equations for many non-trivial examples. Some of these examples are discussed in the paper above.

For future work, we are interested in exploring the proposed research along several directions:

- enrich the programming model to consider nested loops as well as procedure calls,
- take into account guards in conditional statements and loop headers,
- identify other languages to which the ideas here presented apply and which are rich enough to specify properties of data structures such as arrays, records, pointers, etc.
- integrate these and other techniques for mechanically inferring loop invariants, together with theorem proving components, into a tool for program verification.

10 Acknowledgements

The authors would like to thank G. Godoy, R. Nieuwenhuis and A. Oliveras for their help and wise pieces of advice.

References


A Powers of solvable mappings

First of all we need the following lemma, which describes the form of the solutions of the recurrences that arise when computing powers of solvable mappings:

Lemma 21. Consider a recurrence

\[
\begin{pmatrix}
  x_1^{(s+1)} \\
  \vdots \\
  x_r^{(s+1)}
\end{pmatrix} = M \begin{pmatrix}
  x_1^{(s)} \\
  \vdots \\
  x_r^{(s)}
\end{pmatrix} + Q(s, \bar{y})
\]

where \( M \in \mathbb{Q}^{r \times r} \) is a matrix with rational eigenvalues and \( Q \) is a vector of \( r \) functions of the form \( \sum_{l=1}^{k} Q_l(s, \bar{y}) \mu_l^l \), where for \( 1 \leq l \leq k \), \( Q_l \in \mathbb{Q}[s, \bar{y}] \) and \( \mu_l \in \mathbb{Q} \) (the \( \bar{y} \) variables represent parameters). Then the solutions of the recurrence have the form:

\[
x_j^{(s)} = \sum_{l=1}^{k_j} P_{jl}(s, \bar{y}, \bar{z}^{(0)}) (\gamma_{jl})^l
\]

where for \( 1 \leq j \leq r \), \( 1 \leq l \leq k_j \), \( P_{jl} \in \mathbb{Q}[s, \bar{y}, \bar{z}^{(0)}] \) and the \( \gamma_{jl} \in \mathbb{Q} \) are either the eigenvalues of \( M \) or belong to the set of bases of exponentials in \( \mathbb{Q}(s, \bar{y}) \).
Proof. If $M \in \mathbb{Q}^{r \times r}$ is a matrix with rational eigenvalues, then \( \exists S, J \in \mathbb{Q}^{r \times r} \) such that \( \det(S) \neq 0 \) and \( J = S^{-1}MS \) is the Jordan normal form of \( M \). By making a change of variables and splitting the variables into independent sets, we can assume without loss of generality that \( M \) has the structure of a Jordan block, so that for a certain \( \lambda \in \mathbb{Q} \) eigenvalue of \( M \\
M = \begin{pmatrix} 
\lambda & & \\
1 & \lambda & \\
& \ddots & \ddots \\
& & 1 & \lambda
\end{pmatrix}
\)

Now we use the theory of generating functions, linear recurrences with constant coefficients and rational functions (see [Sta97]). We denote by \( F_j(z) \) the generating function of the sequence \((x_j^{(n)})_{n \in \mathbb{N}}\). Since the components of \( Q(s, \tilde{y}) \) are linear combinations of exponentials with polynomial coefficients, the corresponding generating functions are rational functions with rational coefficients \( G_j(z, \tilde{y})/H_j(z) \) such that the roots of the \( H_j \) are in the set of bases of exponentials in \( Q(s, \tilde{y}) \).

From the recurrence we get the following system of equations for the \( F_j \)'s:
\[
\begin{pmatrix}
F_1(z) \\
\vdots \\
F_r(z)
\end{pmatrix} = M \begin{pmatrix}
F_1(z) \\
\vdots \\
F_r(z)
\end{pmatrix} + \begin{pmatrix}
G_1(z, \tilde{y})/H_1(z) \\
\vdots \\
G_r(z, \tilde{y})/H_r(z)
\end{pmatrix}
\]

The solution to this system is
\[
\begin{pmatrix}
F_1(z) \\
\vdots \\
F_r(z)
\end{pmatrix} = (I - zM)^{-1} \begin{pmatrix}
x_1^{(0)} \\
\vdots \\
x_r^{(0)}
\end{pmatrix} + z \begin{pmatrix}
G_1(z, \tilde{y})/H_1(z) \\
\vdots \\
G_r(z, \tilde{y})/H_r(z)
\end{pmatrix}
\]

where
\[
(I - zM)^{-1} = \begin{pmatrix}
\frac{1}{1-Z\lambda_1} & & \\
\frac{1}{1-Z\lambda_2} & \frac{1}{1-Z\lambda_2} & \\
& \ddots & \ddots \\
& & \frac{1}{1-Z\lambda_2} & \frac{1}{1-Z\lambda_2}
\end{pmatrix}
\]

Therefore, the generating functions \( F_j(z) \) are also rational functions with poles either in the eigenvalues of \( M \) or in the set of bases of exponentials in \( Q(s, \tilde{y}) \). From the theory of rational generating functions, we get that the solutions to the recurrence have the form as in the statement of the lemma.

\[ \square \]

Now we are able to describe the form of the general powers of solvable mappings, using the equivalence of computing powers and solving recurrences:
Theorem 3. Let \( g \in \mathbb{Q}[\hat{z}]^m \) be a solvable mapping with rational eigenvalues. Then for \( 1 \leq j \leq m \) \( g_j^l(\hat{z}) \), the \( j \)-th component of \( g^l(\hat{z}) \), can be expressed as

\[
g_j^l(\hat{z}) = \sum_{i=1}^{k_j} P_{ji}(s, \hat{z})(\gamma_{ji})^s, \quad 1 \leq j \leq m, \quad s \geq 0
\]

where for \( 1 \leq j \leq m \), \( 1 \leq l \leq k_j \), \( P_{ji} \in \mathbb{Q}[s, \hat{z}] \) and \( \gamma_{ji} \in \mathbb{Q} \). Moreover, the \( \gamma_{ji} \) are products of the eigenvalues of \( g \).

Proof. It is clear that the statement is equivalent to showing the following. Given a solvable mapping with rational eigenvalues \( g \in \mathbb{Q}[\hat{z}]^m \), we have to prove that the general solution of the recurrence \( \hat{z}^{l+i} = g(\hat{z}^i) \) has the form for \( 1 \leq j \leq m \):

\[
x_j^{(s)} = \sum_{i=1}^{k_j} P_{ji}(s, \hat{z}^{(0)})(\gamma_{ji})^s, \quad 1 \leq j \leq m, \quad s \geq 0
\]

where for \( 1 \leq j \leq m \), \( 1 \leq l \leq k_j \), \( P_{ji} \in \mathbb{Q}[s, \hat{z}^{(0)}] \) and \( \gamma_{ji} \in \mathbb{Q} \); we also have to show that the \( \gamma_{ji} \) are products of the eigenvalues of \( g \).

Since \( g \) is solvable with rational eigenvalues, there exists a partition of the set of variables \( \hat{z}, \hat{z} = \bigcup_{i=1}^{k} U_i \) with \( U_i \cap U_j = \emptyset \) if \( i \neq j \), such that \( \forall i : 1 \leq i \leq k \) we have

\[
g_{U_i}(\hat{z}) = M_i U_i^T + P_i(U_1, \ldots, U_{i-1})
\]

where \( M_i \in \mathbb{Q}[U_i \times [r_i]] \) is a matrix with rational eigenvalues and \( P_i \) is a vector of \( [U_i] \) polynomials with coefficients in \( \mathbb{Q} \) and depending on the variables in \( U_1, \ldots, U_{i-1} \).

Let us prove the theorem by induction on \( i \), the counter of the sets in the partition. By renaming the variables, we can assume without loss of generality that there exist \( 0 = r_0 \leq r_1 \leq r_2 \leq \cdots \leq r_k = m \) such that \( \forall i : 1 \leq i \leq k \) \( U_i = \{x_{r_{i-1}+1}, x_{r_{i-1}+2}, \ldots, x_{r_i}\} \).

For \( i = 0 \) we want to prove that \( \forall x_j \) with \( 1 \leq j \leq r_1 \), \( x_j^{(s)} \) has the form like in the statement. For the first \( r_1 \) variables we have the recurrence:

\[
\begin{pmatrix}
x_1^{(s+1)} \\
\vdots \\
x_{r_1}^{(s+1)}
\end{pmatrix} = M_1 \begin{pmatrix}
x_1^{(s)} \\
\vdots \\
x_{r_1}^{(s)}
\end{pmatrix} + P_1
\]

where \( M_1 \) is a matrix with rational eigenvalues and \( P_1 \) is a constant vector. By Lemma 21, the \( x_j^{(s)} \) have the desired form for \( 1 \leq j \leq r_1 \). Moreover, since \( P_1 \) is constant, for \( 1 \leq j \leq r_1 \) the bases of exponentials in \( x_j^{(s)} \) are eigenvalues of \( M_1 \), and therefore eigenvalues of \( g \).

Now for \( i > 0 \) we have the recurrence:

\[
\begin{pmatrix}
x_{r_{i-1}+1}^{(s+1)} \\
\vdots \\
x_{r_i}^{(s+1)}
\end{pmatrix} = M_i \begin{pmatrix}
x_{r_{i-1}+1}^{(s)} \\
\vdots \\
x_{r_i}^{(s)}
\end{pmatrix} + P_i(x_1^{(s)}, \ldots, x_{r_{i-1}}^{(s)})
\]
By induction hypothesis, \( \forall j : 1 \leq j \leq r_{i-1} \) \( x_j^{(e)} \) has the form like in the statement. Therefore, if \( \forall j : 1 \leq j \leq r_{i-1} \) we plug the solution \( x_j^{(e)} \) in \( P_i(x_1^{(e)}, ..., x_{r_{i-1}}^{(e)}) \), we get that \( P_i(x_1^{(e)}, ..., x_{r_{i-1}}^{(e)}) \) is a vector of functions of the form

\[
\sum_{i=1}^{k} Q_i(s, x_1^{(0)}, ..., x_{r_{i-1}}^{(0)}) \mu_i
\]

where for \( 1 \leq l \leq k \), \( Q_l \in \mathbb{Q}[s, x_1^{(0)}, ..., x_{r_{i-1}}^{(0)}] \) and \( \mu_i \in \mathbb{Q} \) are products of eigenvalues of \( g \), since \( \forall j : 1 \leq j \leq r_{i-1} \) the bases of exponentials in the solutions \( x_j^{(e)} \) are products of eigenvalues of \( g \). By Lemma 21 again, \( \forall j : r_{i-1} < j \leq r_i \) the \( x_j^{(e)} \) have the required form, and the bases of exponentials appearing in them are either eigenvalues of \( M_i \) or bases of exponentials in \( P_i(x_1^{(e)}, ..., x_{r_{i-1}}^{(e)}) \); in any case, they are products of eigenvalues of \( g \), which is what we wanted to see.

\[\square\]

**B Proof of \( \langle L \rangle = \mathcal{L} \)**

**Proposition 7.** Let \( \Lambda = \{\lambda_1, ..., \lambda_k\} \subset \mathbb{N} \) be a finite set of prime numbers, \( \mathcal{L} = \{l \in \mathbb{Q}[\bar{s}, \bar{u}, \bar{v}] \mid l(t, \bar{x}, \bar{X}, -t) = 0 \ \forall t \in \mathbb{N}\} \) be the set of polynomial relations between the powers of these numbers, and \( L = \{u_1v_1 - 1, ..., u_kv_k - 1\} \). Then \( \langle L \rangle_{\mathbb{Q}[t, \bar{u}, \bar{v}]} = \mathcal{L} \)

**Proof.** Obviously, \( \langle L \rangle \subseteq \mathcal{L} \). Now let us prove the other inclusion. Let \( l \in \mathcal{L} \). Let us take any monomial ordering > and let us divide \( l \) into \( L \). Then we get polynomials \( r, p_1, ..., p_k \in \mathbb{Q}[\bar{s}, \bar{u}, \bar{v}] \) such that

\[
l(s, \bar{u}, \bar{v}) = r(s, \bar{u}, \bar{v}) + \sum_{i=1}^{k} p_i(s, \bar{u}, \bar{v}) \cdot (u_iv_i - 1)
\]

We want to show that \( r = 0 \). Let us assume that \( r \neq 0 \) and we will get a contradiction. We can write

\[
r(s, \bar{u}, \bar{v}) = \sum_{\sigma, \beta \in \mathbb{N}^k} P_{\sigma, \beta}(s) \bar{u}^\sigma \bar{v}^\beta
\]

where \( \bar{u}^\sigma = \prod_{i=1}^{k} u_i^{\sigma_i}, \bar{v}^\beta = \prod_{i=1}^{k} v_i^{\beta_i} \) and \( P_{\sigma, \beta} \in \mathbb{Q}[s] \) are polynomials such that at least one of them is not null, and only finitely many of them are not null.

Then \( \forall t \in \mathbb{N} \) we have that

\[
0 = l(t, \bar{x}, \bar{X}, -t) = r(t, \bar{x}, \bar{X}, -t) = \sum_{\sigma, \beta \in \mathbb{N}^k} P_{\sigma, \beta}(t) \prod_{i=1}^{k} \lambda_i^{(\sigma_i - \beta_i)t}
\]

Given \( \bar{\xi}, \bar{\beta} \in \mathbb{N}^k \), let us define \( \lambda_{\sigma, \beta} = \prod_{i=1}^{k} \lambda_i^{\sigma_i - \beta_i} \). Then the above equation can be expressed as \( \forall t \in \mathbb{N} \)

\[
0 = \sum_{\sigma, \beta \in \mathbb{N}^k} P_{\sigma, \beta}(t) \lambda_{\sigma, \beta}
\]
Now let us see that if \((\tilde{\alpha}, \tilde{\beta}) \neq (\tilde{\gamma}, \tilde{\delta})\), then \(\lambda_{\tilde{\alpha}, \tilde{\beta}} \neq \lambda_{\tilde{\gamma}, \tilde{\delta}}\). Let us assume the contrary, i.e., that \(\lambda_{\tilde{\alpha}, \tilde{\beta}} = \lambda_{\tilde{\gamma}, \tilde{\delta}}\) and we will get a contradiction. If \(\lambda_{\tilde{\alpha}, \tilde{\beta}} = \lambda_{\tilde{\gamma}, \tilde{\delta}}\), then
\[
\prod_{i=1}^{k} \lambda_{i}^{\alpha_{i} - \beta_{i} - \gamma_{i} + \delta_{i}} = 1.
\]
As the \(\lambda_{i}\)s are different prime numbers, we necessarily have that \(\alpha_{i} - \beta_{i} - \gamma_{i} + \delta_{i} = 0\) for \(1 \leq i \leq k\). Moreover, since no monomial of \(r\) can be divided by the \(v_{1}v_{2}\)s by the properties of the division algorithm, either \(\alpha_{i} = 0\) or \(\beta_{i} = 0\), and either \(\gamma_{i} = 0\) or \(\delta_{i} = 0\). If \(\alpha_{i} = 0\), then \(\beta_{i} = \delta_{i} - \gamma_{i}\), and as \(\beta_{i} \geq 0\) and either \(\gamma_{i} = 0\) or \(\delta_{i} = 0\), we get that \(0 = \gamma_{i} = \alpha_{i}\) and \(\beta_{i} = \delta_{i}\). The case \(\delta_{i} = 0\) is symmetric. So \(\lambda_{\tilde{\alpha}, \tilde{\beta}} = \lambda_{\tilde{\gamma}, \tilde{\delta}}\) implies \((\tilde{\alpha}, \tilde{\beta}) = (\tilde{\gamma}, \tilde{\delta})\).

Let \(\tilde{\alpha}^{*}, \tilde{\beta}^{*} \in \mathbb{N}^{k}\) be such that
\[
\lambda_{\tilde{\alpha}^{*}, \tilde{\beta}^{*}} = \max \{ \lambda_{\tilde{\alpha}, \tilde{\beta}} | P_{\tilde{\alpha}, \tilde{\beta}} \neq 0 \}
\]
Notice that \(\tilde{\alpha}^{*}, \tilde{\beta}^{*}\) are well defined, since \(r \neq 0\) by hypothesis. By definition, and as \((\tilde{\alpha}, \tilde{\beta}) \neq (\tilde{\gamma}, \tilde{\delta})\) implies \(\lambda_{\tilde{\alpha}, \tilde{\beta}} \neq \lambda_{\tilde{\gamma}, \tilde{\delta}}\), we have that \((\tilde{\alpha}, \tilde{\beta}) \neq (\tilde{\alpha}^{*}, \tilde{\beta}^{*})\) implies \(\lambda_{\tilde{\alpha}, \tilde{\beta}} < \lambda_{\tilde{\alpha}^{*}, \tilde{\beta}^{*}}\).

Now we divide into \((\lambda_{\tilde{\alpha}, \tilde{\beta}})^{t}\) and get that \(\forall t \in \mathbb{N}\)
\[
0 = \sum_{\tilde{\alpha}, \tilde{\beta} \in \mathbb{N}^{k}} P_{\tilde{\alpha}, \tilde{\beta}}(t) \left( \frac{\lambda_{\tilde{\alpha}, \tilde{\beta}}}{\lambda_{\tilde{\alpha}^{*}, \tilde{\beta}^{*}}} \right)^{t}
\]
Taking limits,
\[
0 = \lim_{t \to \infty} P_{\tilde{\alpha}^{*}, \tilde{\beta}^{*}}(t)
\]
which is in contradiction with the fact that \(P_{\tilde{\alpha}^{*}, \tilde{\beta}^{*}} \neq 0\).

\[\square\]

### C Correctness and Completeness of the Implementation

First of all, we need the following technical lemma. It intuitively means that \(F_{i}(-s, \tilde{u}, \tilde{v}, \cdot)\) and \(F_{i}(s, \tilde{u}, \tilde{v}, \cdot)\) are “inverses modulo \(\langle L \rangle\)”:  

**Lemma 22.** For \(1 \leq i \leq n\) and \(\forall q \in \mathbb{Q}[\tilde{x}, \tilde{x}^{*}]\) we have that
\[
q(\tilde{x}, \tilde{x}^{*}) - q(F_{i}(s, \tilde{u}, \tilde{v}, F_{i}(-s, \tilde{v}, \tilde{u}, \tilde{x})), \tilde{x}^{*}) \in \langle L \rangle \mathbb{Q}[\tilde{x}, \tilde{x}^{*}].
\]

**Proof.** We can write
\[
q(\tilde{x}, \tilde{x}^{*}) - q(F_{i}(s, \tilde{u}, \tilde{v}, F_{i}(-s, \tilde{v}, \tilde{u}, \tilde{x})), \tilde{x}^{*}) =
\]
\[
= \sum_{\alpha, \beta \in \mathbb{N}^{m}} R_{\alpha, \beta}(s, \tilde{u}, \tilde{v})(\tilde{x})^{\alpha}(\tilde{x}^{*})^{\beta}
\]
where \((\tilde{x})^{\alpha} = \prod_{j=1}^{m} x_{j}^{\alpha_{j}}\), \((\tilde{x}^{*})^{\beta} = \prod_{j=1}^{m} (x_{j})^{\beta_{j}}\) and \(R_{\alpha, \beta} \in \mathbb{Q}[s, \tilde{u}, \tilde{v}]\) are polynomials such that only a finite number of them are different from 0. Then \(\forall t \in \mathbb{N}\)
\[
q(\tilde{x}, \tilde{x}^{*}) - q(F_{i}(t, \tilde{x}, \tilde{x}^{*}, F_{i}(-t, \tilde{x}, \tilde{x})), \tilde{x}^{*}) =
\]
\[ q(\hat{x}, \hat{x}^*) - q(f_i^j(f_i^{-j}(\hat{x})), \hat{x}^*) = q(\hat{x}, \hat{x}^*) - q(\hat{x}, \hat{x}^*) = 0 \]

Therefore \( \forall t \in \mathbb{N} \) we have

\[
\sum_{\alpha, \beta \in \mathbb{N}^m} R_{\alpha, \beta}(t, \lambda^t, \lambda^{-t})(\hat{x})\beta(\hat{x}^*)^\beta = 0
\]

which implies that \( \forall \alpha, \beta \in \mathbb{N}^m \ R_{\alpha, \beta} \in \mathcal{L} = \langle L \rangle_{\mathbb{Q}[\sigma, \pi, \tau]} \). Thus

\[
q(\hat{x}, \hat{x}^*) - q(F_i(s, \bar{u}, \bar{v}, F_i(-s, \bar{u}, \bar{v}, \hat{x})), \hat{x}^*) \in \langle L \rangle_{\mathbb{Q}[\sigma, \pi, \tau, \bar{x}^*]}
\]

\[ \square \]

The following result intuitively means that we do not lose invariant polynomials in our approximation, and so we maintain completeness:

**Proposition 8.** \( P_\infty \subseteq \langle S \rangle_{\mathbb{Q}[\sigma, \pi, \tau]} \) is invariant in the implementation.

**Proof.** Let us see that the inclusion holds at the beginning. If \( p \in P_\infty \), taking \( \sigma = \lambda \ \forall \alpha^* \in \forall(\langle S_0 \rangle) \ p(\alpha^*, \alpha^*) = 0 \), and so

\[
p \in \forall(\langle \bigcup_{j=1}^m \{x_j - x_j^*\} \bigcup \langle S_0 \rangle \rangle)
\]

But as \( \langle S_0 \rangle = \forall(\langle S_0 \rangle) \), by Lemma 11

\[
\forall(\langle \bigcup_{j=1}^m \{x_j - x_j^*\} \bigcup \langle S_0 \rangle \rangle) = \langle \bigcup_{j=1}^m \{x_j - x_j^*\} \bigcup S_0 \rangle
\]

and thus

\[
p \in \langle \bigcup_{j=1}^m \{x_j - x_j^*\} \bigcup S_0 \rangle
\]

Now it remains to be seen that the inclusion is preserved at each iteration. From now on, \( \langle \cdot \rangle \) means \( \langle \cdot \rangle_{\mathbb{Q}[\sigma, \pi, \tau, \bar{x}^*]} \). It suffices to see that

\[
P_\infty \subseteq \langle L \cup \bigcap_{i=1}^n \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle
\]

since by definition \( P_\infty \subseteq \mathbb{Q}[\bar{x}, \bar{x}^*] \). But

\[
\langle L \cup \bigcap_{i=1}^n \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle = \bigcap_{i=1}^n \langle L \cup \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle
\]

So for \( 1 \leq i \leq n \) we have to see that

\[
P_\infty \subseteq \langle L \cup \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle
\]
Let $P = \{p_1, ..., p_k\} \subset P_\infty$ be a Gröbner basis for $P_\infty$. Let $q \in P_\infty$. We want to show that

$$q \in \langle L \cup \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle$$

First, let us see $q(F_i(s, \bar{u}, \bar{v}, \bar{x}), \bar{x}^*) \in \langle L \cup P_\infty \rangle$. If we divide $q(F_i(s, \bar{u}, \bar{v}, \bar{x}), \bar{x}^*)$ into $p_1, ..., p_k$ with respect to any monomial ordering $\succ$, we get $R, Q_1, ..., Q_k \in \mathbb{Q}[s, \bar{u}, \bar{v}, \bar{x}, \bar{x}^*]$ such that

$$q(F_i(s, \bar{u}, \bar{v}, \bar{x}), \bar{x}^*) = R + \sum_{j=1}^{k} Q_j p_j$$

We want to show that $R \in \langle L \rangle$.

Since $q \in P_\infty$, it is easy to see that $\forall t \in \mathbb{N}$

$$q(F_i(t, \bar{x}^t, \bar{x}^{-t}, \bar{x}), \bar{x}^*) = q(f^t_i(\bar{x}), \bar{x}^*) \in P_\infty$$

But the remainder obtained when dividing $q(f^t_i(\bar{x}), \bar{x}^*) \in P_\infty$ into $p_1, ..., p_k$ is 0. As $p_1, ..., p_k$ is a Gröbner basis, it can be proved that $\forall t \in \mathbb{N}$

$$R(t, \bar{x}^t, \bar{x}^{-t}, \bar{x}, \bar{x}^*) = 0$$

We write $R(s, \bar{u}, \bar{v}, \bar{x}, \bar{x}^*) = \sum_{\sigma, \beta \in \mathbb{N}} R_{\sigma, \beta}(s, \bar{u}, \bar{v})(\bar{x})^\sigma(\bar{x}^*)^\beta$, where $(\bar{x})^\sigma = \prod_{j=1}^{m} x_j^{a_{j, \sigma}}$, $(\bar{x}^*)^\beta = \prod_{j=1}^{m} (x_j^*)^{b_{j, \beta}}$ and $R_{\sigma, \beta} \in \mathbb{Q}[s, \bar{u}, \bar{v}]$ are polynomials such that only a finite number of them are different from 0. We have that $\forall t \in \mathbb{N}$

$$0 = R(t, \bar{x}^t, \bar{x}^{-t}, \bar{x}, \bar{x}^*) = \sum_{\sigma, \beta \in \mathbb{N}} R_{\sigma, \beta}(t, \bar{x}^t, \bar{x}^{-t})(\bar{x})^\sigma(\bar{x}^*)^\beta$$

So $\forall t, \bar{\beta} \in \mathbb{N}^m$ and $\forall t \in \mathbb{N}$ we get that $R_{\sigma, \bar{\beta}}(t, \bar{x}^t, \bar{x}^{-t}) = 0$, i.e $R_{\sigma, \bar{\beta}} \in L = \langle L \rangle_{[\bar{x}, \bar{x}^t]}$. Thus $R \in \langle L \rangle$ and $q(F_i(s, \bar{u}, \bar{v}, \bar{x}), \bar{x}^*) \in \langle L \cup P_\infty \rangle$.

Since $q(F_i(s, \bar{u}, \bar{v}, \bar{x}), \bar{x}^*) \in \langle L \cup P_\infty \rangle$ and $L \subset \mathbb{Q}[s, \bar{u}, \bar{v}]$, substituting $\bar{x}$ by $F_i(-s, \bar{v}, \bar{u}, \bar{x})$

$$q(F_i(s, \bar{u}, \bar{v}, F_i(-s, \bar{v}, \bar{u}, \bar{x})), \bar{x}^*) \in \langle L \cup \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle$$

From Lemma 22

$$q(\bar{x}, \bar{x}^*) - q(F_i(s, \bar{u}, \bar{v}, F_i(-s, \bar{v}, \bar{u}, \bar{x})), \bar{x}^*) \in \langle L \rangle$$

So $q(\bar{x}, \bar{x}^*) \in \langle L \cup \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), P_\infty) \rangle$, which is what we wanted to see.

□

Finally, the last theorem implies trivially that the implementation is correct and complete:

**Theorem 4.** If the procedure terminates with output $I^*$, the implementation terminates in at most the same number of iterations with output $S^*$ such that $\langle S^* \rangle_{[\sigma, \sigma^*]} = I^*$. 
Proof. Let us denote by $\mathcal{I}_N$ the ideal stored in the variable $I$ of the loop at the end of the $N$-th iteration in the procedure; and, analogously, let $\mathcal{G}_N$ be the ideal generated by the set of polynomials stored in the variable $S$ at the end of the $N$-th iteration in the implementation.

First of all, we will prove that $\forall N \in \mathbb{N}$ we have $\mathcal{G}_N \subseteq \mathcal{I}_N$. Then the termination of the procedure will imply a chain of equalities that will yield the theorem.

So let us prove that $\forall N \in \mathbb{N}$, $\mathcal{G}_N \subseteq \mathcal{I}_N$ by induction on $N$. If $N = 0$ there is nothing to prove, since by definition $(S_0)_{\mathbb{Q}[x^*]} = I_0$ and so $\mathcal{G}_0 = \mathcal{I}_0$.

If $N > 0$,

$$\mathcal{I}_N = \bigcap_{i=1}^{\infty} \bigcap_{l=1}^{n} \text{subs}(f_{i-1}^{m-1}, \mathcal{I}_{N-1})$$

$$\mathcal{G}_N = \mathbb{Q}[\bar{x}, \bar{x}^*] \cap \left\langle L \cup \left( \bigcap_{i=1}^{n} \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), \mathcal{G}_{N-1}) \right) \right\rangle_{\mathbb{Q}[s, \bar{v}, \bar{u}, \bar{x}, \bar{x}^*]} =$$

$$= \mathbb{Q}[\bar{x}, \bar{x}^*] \cap \left( \bigcap_{i=1}^{n} (L \cup \text{subs}(F_i(-s, \bar{v}, \bar{u}, \cdot), \mathcal{G}_{N-1}))_{\mathbb{Q}[s, \bar{v}, \bar{u}, \bar{x}, \bar{x}^*]} \right)$$

Let $q \in \mathcal{G}_N$. For $1 \leq i \leq n$ and $t \in \mathbb{N}$ we have to show that $q \in \text{subs}(f_{i-1}^{m-1}, \mathcal{I}_{N-1})$.

By induction hypothesis, it is enough to see that $q \in \text{subs}(f_{i-1}^{m-1}, \mathcal{G}_{N-1})$.

Now, if $p_1, \ldots, p_k \in \mathbb{Q}[\bar{x}, \bar{x}^*]$ is a basis for $\mathcal{G}_{N-1}$ and $L = \{u_1 v_1 - 1, \ldots, u_k v_k - 1\}$ as defined in Section 6, there exist polynomials $P_r, L_j \in \mathbb{Q}[s, \bar{v}, \bar{x}, \bar{x}^*]$ for $1 \leq r \leq t$ and $1 \leq j \leq k$ such that

$$q(\bar{x}, \bar{x}^*) = \sum_{r=1}^{i} P_r(s, \bar{v}, \bar{x}, \bar{x}^*) p_r(F_i(-s, \bar{v}, \bar{u}, \bar{x}), \bar{x}^*) +$$

$$+ \sum_{j=1}^{k} L_j(s, \bar{v}, \bar{x}, \bar{x}^*) (u_j v_j - 1)$$

By taking an arbitrary $t \in \mathbb{N}$ and evaluating conveniently the auxiliar variables,

$$q(\bar{x}, \bar{x}^*) = \sum_{r=1}^{i} P_r(t, \bar{x}, \bar{x}^*) p_r(F_i(-s, \bar{v}, \bar{u}, \bar{x}), \bar{x}^*) +$$

$$+ \sum_{j=1}^{k} L_j(t, \bar{x}, \bar{x}^*) (\bar{x}^* - 1) =$$

$$= \sum_{r=1}^{i} P_r(t, \bar{x}, \bar{x}^*) p_r(f_{i-1}(\bar{x}), \bar{x}^*)$$

So $q(\bar{x}, \bar{x}^*) \in \text{subs}(f_{i-1}^{m-1}, \mathcal{G}_{N-1})$ indeed. Therefore $\forall N \in \mathbb{N}$ $\mathcal{G}_N \subseteq \mathcal{I}_N$.

Now, if the procedure terminates in $N$ iterations, then $P^* = \mathcal{I}_N = \mathcal{G}_{N-1}$ for a certain $N \geq 1$, and we have that $\mathcal{G}_{N-1} = P_\infty$. Then, by Proposition 8,
\( \mathcal{S}_{N-1} \subseteq \mathcal{S}_N = \mathcal{S}_N \subseteq P_\infty \subseteq \mathcal{S}_N \). But \( \mathcal{S}_N \subseteq \mathcal{S}_{N-1} \). So \( \mathcal{S}_{N-1} = \mathcal{S}_N = P_\infty = (S^*) = I^* \), and the implementation terminates in at most the same number of iterations as the procedure.

\( \square \)