Computing Approximations of Linear Transition Systems

Julien Musset, Michaël Rusinowitch

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Computing Approximations of Linear Transition Systems

Julien Musset — Michaël Rusinowitch

N° 4774

March 2003

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--4774--FR+ENG

Computing Approximations of Linear Transition Systems

Julien Musset , Michaël Rusinowitch

Thème 2 — Génie logiciel
et calcul symbolique
Projet Cassis

Rapport de recherche n° 4774 — March 2003 — 20 pages

Abstract: Transition systems have been intensively applied to the modelling of complex systems. Their safety properties can be verified using model-checking procedures by iterative computation of fixed points. The approach has to face two main difficulties: the complexity of computations on the data domain and the termination of the iterative algorithm. In many cases an analysis of the transition system can be exploited in order to speed up the calculus. Metatransitions are upper approximations of transition relations: they lead in one step to a superset of the states occuring on an infinite trajectory. Using polynomials we compute metatransitions for linear transition systems. We apply this method to a train controller.

Key-words: infinite systems, model-checking, acceleration rules, linear transition systems, metatransitions

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,

Calcul d'approximations de systèmes de transition linéaires

Résumé : Nous présentons une méthode pour calculer des métatransitions dans le cadre des systèmes de transitions linéaires. La méthode permet d'approcher supérieurement les ensembles accessibles et s'applique à la résolution pratique de problèmes de sûreté.

Mots-clés : systèmes infinis, model-checking, systèmes de transition linéaires, règles d'accélération

1 Introduction

Transition systems [12] have been applied to the modelling of complex systems, for example they have been used for giving semantics to synchronous languages such as LUSTRE [5], SIGNAL [3] or to hybrid automata [14]. Model-checking [6, 18] is a powerful technique for the automatic verification of systems: a model-checking algorithm determines whether a transition system meets a requirement specification that is given as a temporal formula. For discrete finite-state systems model-checking has been successful in validating communication protocols and hardware circuits. In recent years model-checking algorithms have been extended to infinite state systems. As the states cannot be enumerated they have to be represented symbolically. Moreover, proving that a model verifies a temporal formula is undecidable in general.

From the fixedpoint characterization of temporal properties [10], model-checking can be reduced to the successive computations of least or greatest fixed points of monotonous functions over sets of states. For instance, with the help of an observer [13], verifying a safety property is equivalent to verify a reachability property where backward or forward analysis can be employed. To improve verification we need to overcome two main obstacles. Firstly, operations over symbolic representations of sets of states are expensive. Secondly, the computation of the fixed point may not terminate. Several tools allow for improving the fixed point computation: abstraction, that consists in substituting the domain of the concrete states by a simpler domain of abstract states [2], widening and narrowing operators that compute over- and under-approximation of unions and intersections of sets [7]. When the set of states is infinite, the computation of the set of reachable states may not terminate.

In this work we focus on reachability and safety properties. For infinite systems, there exists some classes of systems for which reachability problem is decidable bu their restrictions are too strong to be efficient on real systems. To help the termination, acceleration rules help to compute in one step all the states that can be reached by an infinite trajectory.

Example 1 *Let us consider the following transition system in which the set of states is* $\mathbb{Z}$*,* $\rightarrow$ *is the binary relation over* $\mathbb{Z}$ *such that* $x \rightarrow x+1$ *and the initial state is* 0*. We want to compute the set of the states that can be reached from* 0 *using* $\rightarrow$*. The reachability algorithm computes iteratively the set of states can be reached from the initial state in at most zero step, one step, two steps, three steps,... till it does not produce any new state. For this example, we get the following sequence of sets:*

$$\{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}, \ldots$$

This initial computation leads us to think that this sequence is infinite. As a matter of fact the reachability algorithm will not terminate. One technique that could help us consists in generalizing the transition relation $\rightarrow$*. In the previous example,* $x \overset{n \ times}{\rightarrow} \ldots \rightarrow y$ *is equivalent to* $y = x+n$*. Applying reachability algorithm to the transition relation* $\rightsquigarrow$ *defined by* $x \rightsquigarrow y$ *if and only if* $\exists n \in \mathbb{N}\ y = x+n$ *we get the following finite sequence of sets:*

$$\{0\}, \{0\} \cup \{y \in \mathbb{Z} | 1 \leq y\} = \mathbb{N}.$$

We cannot reach new states from the set $\mathbb{N}$*. Hence* $\mathbb{N}$ *is an upper approximation of the reachability set (of* $\rightarrow$*).*

A more realistic system will be given in the following section. The aim of this work is to propose a method to compute such generalized transition relation when $\rightarrow$ is described with complex or real polynomial functions. We will explain why we need to compute upper approximations. The generalized transition relations will be described using polynomials.

Related works. Enforcing the termination of reachability and proof algorithms has been investigated in different settings. Thomas Henzinger and Vlad Rusu propose to guess the set of reachable states from the first steps of the computation [15]. Giorgio Delzanno and Andreas Podelski improve this idea by using acceleration rules in their model-checking system based on constrained logic programming [8]. The notion of acceleration rules is similar to the notion of metatransitions introduced by Bernard Boigelot in his PhD thesis [4]. Boigelot explains how they can be exploited to improve reachability algorithms. Then the author constructs metatransitions for

different kind of datatypes. With a related approach Ashish Tiwari [20] computes supersets of transitions relations defined by real linear differential equation and applies the technique to prove safety properties of hybrid automatas. Let us note that this approach could be interpreted in automated deduction as a generalization heuristics (e.g. such as the ones proposed by Andrew Ireland and Alan Bundy using rippling, a syntactic simplification heuristics, and information from failures to generalize the property to be proved by induction [16]). Interesting applications of metatransitions to protocol verification can be found in [11].

Our work is directly related to these works. To begin with, we focus on systems with complex or real variables instead of integer ones. Moreover we deal with the cases that cannot be handled exactly and are not considered by Bernard Boigelot. Finally, compared to Ashish Tiwari [20], we rather take into account the global behaviour of the systems in all the dimensions and not only in its eigenspaces.

In Section 2, we define transition systems, safety properties, and introduce algorithms for computing reachability sets. We also present the train controller example. Section 3 recalls some previous works on integer linear systems. Section 4 introduce linear transition systems on complex numbers. Section 5 explain how to derive acceleration rules for such systems (starting from simple ones) and in Section 6, we apply our algorithm to the train controller system.

2 Transition systems and model-checking

The complement of a set Q is denoted by $\overline{Q}$. The set of subsets of Q is denoted by $\mathcal{P}(Q)$. The least fixed point of a monotonous function f from $\mathcal{P}(Q)$ to $\mathcal{P}(Q)$ with the complete partial order $\subseteq$ is denoted by $\mu X.f(X)$. For all binary relations $\rightarrow$, the fact that $(x,y) \in \rightarrow$ is denoted by $x \rightarrow y$. Let Q and R be two sets and E be a subset of $Q \times R$. For all $x \in Q$, $E(x)$ is the set $\{y \in R | (x,y) \in E\}$. Let Q be a set, $\rightarrow$ and $\rightsquigarrow$ be two binary relations over Q. The binary relation $\rightarrow \circ \rightsquigarrow$ is the set $\{(x,z) \in Q^2 |$ there exists y such that $x \rightarrow y \rightsquigarrow z\}$. For all positive integer n, $\stackrel{n}{\rightarrow}$ is defined recursively by $\stackrel{0}{\rightarrow} = \{(x,y) \in Q^2 | x = y\}$ and for all n, $\stackrel{n+1}{\rightarrow} = \rightarrow \circ \stackrel{n}{\rightarrow}$. A binary relation $\rightarrow$ over a set Q is closed if $\rightarrow \circ \rightarrow \subseteq \rightarrow$.

Definition 1 *A* **transition systems** *is a triple $(Q, \rightarrow, I)$ in which: Q is a set whose elements are called* **states**, *$\rightarrow$ is a binary relation over Q, called* **transition relation**, *and $I \subseteq Q$ is a set whose elements are called* **initial states**.

Definition 2 *Let $(Q, \rightarrow, I)$ be a transition system. A* **trajectory** *of $(Q, \rightarrow, I)$ is a sequence of states $(q_i)_{0 \leq i \leq n}, n \in \mathbb{N} \cup \{+\infty\}$, such that $q_0 \in I$ et for all $0 \leq i < n$, $q_i \rightarrow q_{i+1}$.*

A state can be reached by a transition system if there exists a finite trajectory whose last element is this state.

Definition 3 *The* **safety problem** *is the decision problem defined by:*

- **instance:** *a tuple $(Q, \rightarrow, I, F)$ in which $(Q, \rightarrow, I)$ is a transition system and $F \subseteq Q$ is a set whose elements are called* **failure states**;
- **question:** *does some trajectory of $(Q, \rightarrow, I)$ reach a failure state ?*

Definition 4 *Let Q be a set and $\rightarrow$ be a binary relation over Q. The* **post-condition** *operator $\mathrm{post}_{\rightarrow}$ is the function from $\mathcal{P}(Q)$ to $\mathcal{P}(Q)$ defined by:*

$$\mathrm{post}_{\rightarrow}(X) = \{q \in Q | \text{ there exists } q' \in X \text{ such that } q' \rightarrow q\}.$$

For solving the safety problem, model-checking algorithms compute the set of reachable states and check whether it contains a failure state. The set of reachable states is equal to $\bigcup_{i \in \mathbb{N}} \mathrm{post}^i_{\rightarrow}(I)$. As the function $X \mapsto I \cup \mathrm{post}_{\rightarrow}(X)$ is monotonous with respect to the order $\subseteq$, the set of reachable states is the least fixed point $\mu X. I \cup \mathrm{post}^i_{\rightarrow}(X)$. The last equality leads to the Algorithm 1 generally used by model-checking tools.

Algorithm 1: Decision procedure for the safety problem
Input: A transition system $(Q, \to, I)$, a set $F \subseteq Q$
Output: Does some trajectory of $(Q, \to, I)$ reach a state of F
SAFETY$(Q, \to, I, F)$
(1) $X := \emptyset$
(2) $Y := I$
(3) **while** $Y \not\subseteq X$
(4) $X := Y$
(5) $Y := I \cup \text{post}_{\to}(X)$
(6) **if** $X \cap F = \emptyset$ **then return** no
(7) **else return** yes

Remark 1 (Backward strategy) *For an instance $(Q, \to, I, F)$ of the safety problem the backward strategy consists in applying Algorithm 1 to the instance $(Q, \leftarrow, I, F)$ where $x \leftarrow y$ if and only if $y \to x$. The algorithm computes the set of states that may reach a failure test and checks whether an initial states is in this set.*

Example 2 (Train controller) *The train controller example is written in the synchronous reactive language* LUSTRE *[5]. It is introduced and detailed in [1] and [9]. One train is following another, the distance between*

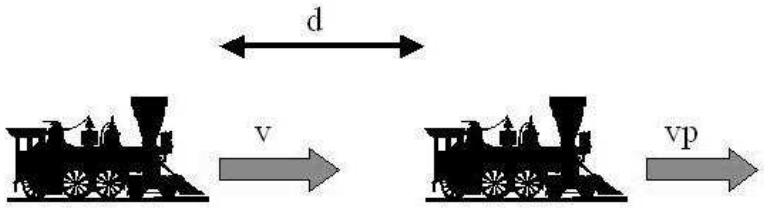

Figure 1: The train controller problem

the two trains is $d(t)$ and its initial value is dinit. The speed of the first train is $vp(t)$. The speed of the second train is $v(t)$ and its acceleration is $a(t)$. The acceleration depends from the mode fu of the train: the train may brake with the constant acceleration $-afu$, elsewhere the acceleration is less or equal than the constant amax. A controller $fu(t)$ decides when the second train has to brake. The goal is to check the correctness of the controller. This problem can be represented using synchronous reactive systems. The following program in LUSTRE *describes the behaviour of the second train:*

```
const afu, amax, dinit;
a = 0 -> if fu then -afu else ap;
v = 0 -> (let vv = (0 -> (pre(v) + a))
          in if vv>=0 then vv else 0);
d = (dinit -> pre(d)) + vp - v;
assert((afu>0) and (ap<amax));
assert((dinit>0) and (vp>=0));
```

Based on LUSTRE *semantics we can express the safety problem as follows. The set of states is $\mathbb{R}^2$, the first coordinate representing the speed of the second train and the second coordinate the distance between the two trains. The transition relation $\to$ is the union of the six transition relations $\to_1, \ldots, \to_6$ defined by:*

- $(v,d) \rightarrow_1 (v',d')$ *iff* $\exists vp\ vp \geq 0, d-v+amax < 0, v-afu \geq 0, a' = afu, v' = v-afu, d' = d+vp-v+afu,$
- $(v,d) \rightarrow_2 (v',d')$ *iff* $\exists vp\ vp \geq 0, d-v+amax < 0, v-afu < 0, a' = afu,\ v' = 0, d' = d+vp$
- $(v,d) \rightarrow_3 (v',d')$ *iff* $\exists vp\ vp \geq 0, v+amax-afu \geq 0, v-afu \geq 0, a' = afu, v' = v-afu, d' = d+vp-v+afu$
- $(v,d) \rightarrow_4 (v',d')$ *iff* $\exists vp\ vp \geq 0, v+amax-afu \geq 0, v-afu < 0, a' = afu, v' = 0, d' = d+vp$
- $(v,d) \rightarrow_5 (v',d')$ *iff* $\exists vp\ am\ vp \geq 0, am < amax, d-v+amax > 0, v+amax-afu < 0, v+am \geq 0, a' = am, v' = v+am, d' = d+vp-v-am$
- $(v,d) \rightarrow_6 (v',d')$ *iff* $\exists vp\ am\ vp \geq 0, am < amax, d-v+amax > 0,\ v+amax-afu < 0, v+am < 0, a' = am, v' = 0, d' = d+vp$

The set of initial states is $\{(v,d) \in \mathbb{R}^2 | v = 0, d > 0\}$. *The set of failure states* F *is* $\{(v,d) \in \mathbb{R}^2 | d \leq 0\}$. *In [1] and [9], backward reachability does not terminate. The authors have to strengthen the property, i.e. to use an upper approximation of the set of failure states. By replacing the set of failure states by the superset:* $\{(v,d) \in \mathbb{R}^2 |\ d \leq 0$ *or* $afu \geq v\}$, *backward reachability terminates and the safety of the controller is proved.* **How could we find automatically such an upper approximation of the failure states ?**

Let us examine more closely the fixedpoint computation. It can be represented as a tree [17]. The root of the tree is associated to the set F. *If the set* X *associated to a node is included in the union of the sets associated to the nodes in the upper levels then the node is a leaf (in black). Otherwise, the node has six children associated respectively to the sets* $\mathrm{post}_{\rightarrow_1}(X), \ldots, \mathrm{post}_{\rightarrow_6}(X)$. *Figure 2 is the proof tree when we apply backward strategy. This tree is infinite because of two infinite branches produced by the transition relations* $\rightarrow_1$ *and* $\rightarrow_3$. *To help the termination, we propose to abstract the* $\rightarrow_1$ *and* $\rightarrow_3$ *and to compute in one step all the states of those infinite branches.*

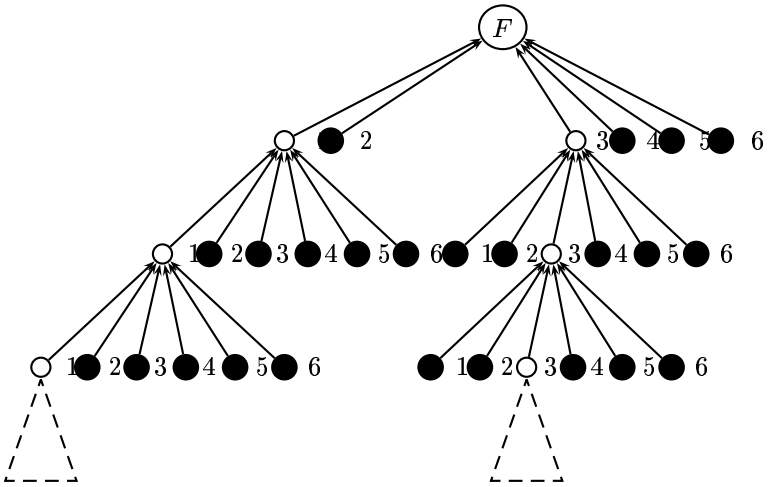

Figure 2: Proof tree for the train controller

3 Linear algebra and integer linear systems

Let p be a strictly positive integer. For all $i \in \{1,\ldots,m\}$, $j \in \{1,\ldots,n\}$, the coefficient in position i,j of an $m \cdot n$ matrix M is denoted by $M_{i,j}$. The vectors are denoted by bold letters such as $\vec{x}$. For all $i \in \{1,\ldots,p\}$, the i^{th} coordinate of a p vector $\vec{x}$ is denoted by $\vec{x}_i$. The identity (resp. zero) matrix of size p is denoted by Id_p (resp. 0_p). A p square matrix N is nilpotent of index n if $N^{n-1} \neq 0_p$ and $N^n = 0_p$. We recall a well-known result from linear algebra:

Theorem 1 (Jordan decomposition) *Let A be a m square complex matrix. The matrix A is similar to a block diagonal matrix $diag(J_1,\ldots,J_n)$ where each J_i is a matrix of the form $\alpha Id_p + N$ where α is a complex number and N is a nilpotent p square complex matrix.*

For all couple of integers $(n,i) \in \mathbb{N}^2$, the binomial coefficient is denoted by $\binom{n}{i}$. For all complex number z, $|z|$ is the norm of z: $|z|^2 = \Re(z)^2 + \Im(z)$.

Definition 5 (Set algebra) *Given a set Q, an algebra on Q is a collection of subsets of Q which is closed under finite unions and complements.*

The set algebra $\mathcal{L}_p(\mathbb{Z})$ is generated by the sets $\{\vec{x} \in \mathbb{Z}^p | {}^t\vec{a}.\vec{x} \geq b\}$ where $\vec{a}$ is a p integer vector and b is an integer number. The set algebra $\mathcal{L}_p(\mathbb{C})$ is generated by the sets $\{\vec{x} \in \mathbb{C}^p | \Re({}^t\vec{a}.\vec{x}) \geq b_r$ and $|\Im({}^t\vec{a}.\vec{x}) \geq b_i\}$ where $\vec{a}$ is a p complex vector and b_r, b_i are real numbers. The set algebra $\mathcal{P}_p(\mathbb{C})$ is generated by the sets $\{\vec{x} \in \mathbb{C}^p | P(\Re(\vec{x}_1),\ldots,\Re(\vec{x}_p),\Im(\vec{x}_1),\ldots,\Im(\vec{x}_1)) \geq 0\}$ where $P(X_1,\ldots,X_{2p})$ is a real polynomial.

3.1 Metatransitions for integer linear systems

Giorgio Delzanno and Andreas Podelski use acceleration rules in their model-checking system based on constrained logic programming [8]. The following transition system illustrates their idea:

- the set of states Q is $\mathbb{Z}^2$,
- the transition relation $\rightarrow$ is defined by $\vec{x} \rightarrow \vec{y}$ if and only if $\vec{x} = \vec{y} - \binom{0}{1}$,
- the set of initial states I is $\{\vec{x} \in \mathbb{Z}^2 | \vec{x}_1 \leq \vec{x}_2\}$.

Using a reachability algorithm, we get this following sequence of sets:

$$\{\vec{x} \in \mathbb{Z}^2 | \vec{x}_1 \leq \vec{x}_2\}, \{\vec{x} \in \mathbb{Z}^2 | \vec{x}_1 \leq \vec{x}_2 + 1\}, \{\vec{x} \in \mathbb{Z}^2 | \vec{x}_1 \leq \vec{x}_2 + 2\}, \ldots$$

The limit set is $\mathbb{Z}^2$. We can derive this result although this fixpoint computation is non-terminating. Let us notice that for all positive integers n, $\vec{x} \rightarrow^n \vec{y}$ is equivalent to $\vec{y} = \vec{x} - \binom{0}{n}$. The set of reachable states is equal to

$$\begin{aligned}\bigcup_{n\in\mathbb{N}} \text{post}^n_{\rightarrow}(I) = \bigcup_{n\in\mathbb{N}} \text{post}_{\overset{n}{\rightarrow}}(I) &= \bigcup_{n\in\mathbb{N}} \{\vec{x} \in \mathbb{Z}^2 | \vec{x}_1 \leq \vec{x}_2 + n\} \\ &= \{\vec{x} \in \mathbb{Z}^2 | \text{ there exists } n \in \mathbb{N} \text{ such that } \vec{x}_1 \leq \vec{x}_2 + n\} \\ &= \{\vec{x} \in \mathbb{Z}^2 | \textbf{true} \} = \mathbb{Z}^2.\end{aligned}$$

The authors describe four accelerations rules using this idea. Assume that the set of states is $\mathbb{Z}^p$ where p is a strictly positive integer. For instance, the rule corresponding to the previous example is defined for all integers i and j in $\{1,\ldots,p\}$ by:

$$\frac{\begin{array}{c}\rightarrow = \rightsquigarrow \cup \rightsquigarrow' \\ \{\vec{x} \in \mathbb{Z}^p | \vec{x}_i \leq \vec{x}_j\} \cap I' \subseteq I \\ I' \subseteq \text{post}_{\rightsquigarrow}(I') \\ \vec{x} \rightsquigarrow \vec{y} \text{ implies } \vec{y}_i = \vec{x}_i + c_i \text{ and } \vec{y}_j = \vec{x}_j + c_j \text{ where } c_j - c_i > 0\end{array}}{I' \subseteq \text{post}_{\rightarrow}(I)}$$

This rule constructs the set of reachable states from the set $\{\vec{x} \in \mathbb{Z}^p | \vec{x}_i \leq \vec{x}_j\} \cap I'$ using the transition relation $\rightsquigarrow$. The authors note that these rules may be generalized to handle more complex sets and transition relations.

In his PhD thesis [4], Bernard Boigelot proposes such a generalization. The set of states is still $\mathbb{Z}^p$. One of his main results is a characterization of the transition relations such that the set of reachable states is in $\mathcal{L}_p(\mathbb{Z})$ if the sets of initial states is in $\mathcal{L}_p(\mathbb{Z})$:

Theorem 2 *Let A be a p square integer matrix, $\vec{b}$ be a p integer vector and let $\rightarrow$ be the transition relation on $\mathbb{Z}^p$ such that $\vec{x} \rightarrow \vec{y}$ if and only if $\vec{y} = A\vec{x} + \vec{b}$. The two following properties are equivalent:*

(i) for all set I of $\mathcal{L}_p(\mathbb{Z})$, the set of the reachable states of the transition system $(\mathbb{Z}^p, \rightarrow, I)$ is in $\mathcal{L}_p(\mathbb{Z})$;

(ii) there exists an integer m strictly positive such that the matrix A^m is similar to a block diagonal matrix of the form $diag(Id_{p_1}, 0_{p_2})$ [1].

The proof constructs the transitive closure of the transition relation $\rightarrow$. Commenting the cases that are not covered by the condition (ii) of Theorem 2, B. Boigelot remarks that:

> **[note page 237]** *Intuitively, the difficulty originates from the fact that, if a linear (transition relation $\rightarrow$) does not verify the hypothesis of Theorem 2 then the trajectory ($\bigcup_{n\in\mathbb{N}} \mathrm{post}^n_{\rightarrow}(\{\vec{x}\})$) of an individual vector value $\vec{x} \in \mathbb{Z}^p$ to which $\rightarrow$ is repeatedly applied is in general non linear. This makes a manageable description of* $\mathrm{post}^*_{\rightarrow}(S)$*, for a subset S of $\mathbb{Z}^p$, much more difficult to obtain.*

This is the problem we try to tackle in this paper.

4 Complex transition systems

In this work, we focus on complex systems, i.e. transitions systems of type $(\mathbb{C}^p, \rightarrow, I)$, where $\rightarrow$ is in $\mathcal{P}_{2p}(\mathbb{C})$ and I is in $\mathcal{P}_p(\mathbb{C})$. Real linear systems are handled as special cases of complex linear systems. It is interesting to abstract integer linear systems into real ones since solving integer systems is more expensive than solving real (or complex) ones. We discuss here how this abstraction can be performed. Then we present the differences between our approach and the previous works we have described.

4.1 From integer systems to real systems

We define inductively the projection mapping $\gamma : \mathcal{L}_p(\mathbb{Z}) \mapsto \mathcal{L}_p(\mathbb{R})$ by:

- $\gamma(\{\vec{x} \in \mathbb{Z}^p | {}^t\vec{a} \cdot \vec{x} \geq b\}) = \{\vec{x} \in \mathbb{R}^p | {}^t\vec{a} \cdot \vec{x} \geq b\}$ where $\vec{a}$ is a p integer vector and b is an integer number,
- $\gamma(X \cup Y) = \gamma(X) \cup \gamma(Y)$ and $\gamma(\overline{X}) = \overline{\gamma(X)}$.

The mapping γ is extended to instances of the safety problem:

$$\gamma((\mathbb{Z}^p, \rightarrow, I, F)) = (\mathbb{R}^p, \gamma(\rightarrow), \gamma(I), \gamma(F)).$$

This abstraction is motivated by the fact that verifying linear formulas is more complex with integers than with reals [19]. Checking whether

$$\{\vec{x} \in \mathbb{K}^p |\ {}^t\vec{a} \cdot \vec{x} \geq b\} \subseteq \{\vec{x} \in \mathbb{K}^p |\ {}^t\vec{a} \cdot \vec{x} \geq b\}$$

where $\vec{a} \in \mathbb{K}^p$ and $b \in \mathbb{K}$ is NP-complete if $\mathbb{K} = \mathbb{Z}$ whereas it is polynomial if $\mathbb{K} = \mathbb{R}$. This result leads designers of model-checking algorithms to weaken the comparison test between sets of states by abstracting the integers sets into reals sets. In [8], Giorgio Delzanno and Andreas Podelski describe a class of sets for which the abstraction gives an exact result (i.e. the same result). The following proposition is another correctness result that could be applied to backward strategies.

[1] the notation $diag(b_1, \ldots, b_l)$ means that $b_1, \ldots, b_l$ are the blocks on the main diagonal

Proposition 1 *Let $(Q, \rightarrow, I, F)$ be an instance of the safety problem, let Q' and I' be two sets such that $Q \subseteq Q'$, $I \subseteq I' \subseteq Q'$ and $(I' \setminus I) \cap Q = \emptyset$. Let $\rightsquigarrow$ be a binary relation over Q' such that $\rightarrow \subseteq \rightsquigarrow$ and for all $x \in Q$, $y \rightsquigarrow x$ implies $y \in Q$ and $y \rightarrow x$. The two instances $(Q, \rightarrow, I, F)$ and $(Q', \rightsquigarrow, I', F)$ of the safety problem have the same answer.*

Proposition 1 can be applied easily in backward strategy when an integer transition system is abstracted into a real one. In the abstracted system, the successive states of an integer state is always an integer state. The main condition of Proposition 1 is verified.

Example 3 *The set of states is $\mathbb{Z}$ and the transition relation $\rightarrow$ is defined by $x \rightarrow P(x)$ where P is an integer polynomial. Let I and F be two subsets of $\mathbb{Z}$. Proposition 1 implies that $I \cap \mathrm{pre}_{\rightarrow}(F) = \emptyset$ is equivalent to $I \cap \mathrm{pre}_{\gamma(\rightarrow)}(\gamma(F)) = \emptyset$.*

4.2 Nonlinear trajectories

We adapt Theorem 2 of Bernard Boigelot for complex (and real) transition systems.

Theorem 3 *Let A be a p square complex matrix, $\vec{b}$ be a p vector and $\rightarrow$ be the transition relation on $\mathbb{C}^p$ such that $\vec{x} \rightarrow \vec{y}$ if and only if $\vec{y} = A\vec{x} + \vec{b}$. The two following properties are equivalent:*

(i) for all set I of $\mathcal{L}_p(\mathbb{C})$, there exists a set E of $\mathcal{L}_{p+1}(\mathbb{C})$ such that

$$\mathrm{post}_{\rightarrow}(I) = \bigcup_{n \in \mathbb{N}} E(n),$$

(ii) there exists a strictly positive integer m such that A^m is similar to a block diagonal matrix of the form $diag(Id_{p_1}, 0_{p_2})$.

From this result we can draw two consequences. First, as our sets of states are represented with complex or real variables, we wont be able in general to compute exactly the set of reachable states. Second, we will have to apply different approximations schemes according to the system behaviour which depends from the eigenvalues of the transition relation matrix A. Consequently, given a transition relation $\rightarrow$, we shall construct a transition relation $\rightsquigarrow$ such that $\rightarrow \subseteq \rightsquigarrow$ and $\rightsquigarrow \circ \rightsquigarrow \subseteq \rightsquigarrow$. These conditions implies that $\rightsquigarrow$ contains $\stackrel{n}{\rightarrow}$ for all $n \in \mathbb{N}$ and that we get in one step of Algorithm 1 all the states that can be reached using the transition relation $\rightsquigarrow$.

5 Computing metatransitions

We first describe our general approach to build good approximations of transition systems. The set of states we consider are subsets of $\mathbb{C}^p$, $p > 0$. We will study transition relations $\rightarrow$ of the form:

$$\vec{x} \rightarrow \vec{y} \text{ if and only if there exists } \vec{z} \text{ such that } \vec{y} = A\vec{x} + A'\vec{z} + \vec{b} \text{ and } (\vec{x}, \vec{z}) \in C$$

where A and A' are complex p square matrices, $\vec{b}$ is a complex p vector and C is a set in $\mathcal{P}_{2p}(\mathbb{C})$. We are looking for a closed superset of $\rightarrow$. To compute such a transition relation, we introduce a variable n as suggested by Theorem 3.

Proposition 2 *Let $\rightarrow$ be a transition relation over $Q \subseteq \mathbb{C}^p$, and let E be a set of $\mathcal{P}_{2p+1}(\mathbb{C})$ such that $E(1)$ contains $\rightarrow$ and for all integer m and n greater than 1, $E(m) \circ E(n) \subseteq E(m+n)$. Then $\bigcup_{n \in \mathbb{R}, n \geq 1} E(n)$ contains $\rightarrow$ an d is closed.*

In the following, we will say that E is an **approximation set for** $\rightarrow$.

We want to construct such a set E. We begin with the simplest transition relations of the form $\vec{x} \rightarrow \vec{y}$ *if and only if* $\vec{y} = (\alpha Id_p + N)\vec{x}$ to finish with the most general transition relations $\vec{x} \rightarrow \vec{y}$ *if and only if there exists* $\vec{z}$ *such* $A\vec{x} + A'\vec{z} + \vec{b}$ *and* $(\vec{x}, \vec{z}) \in C$.

5.1 Simple cases

In this part, we consider the transition relation of the form:

$$\vec{x} \to \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x} + \vec{b}$$

where α is a complex number, N is a nilpotent p square matrix and $\vec{b}$ is a p vector. There are three base cases: $\alpha = 0$ and $\vec{b} = \vec{0}$, $\alpha = 1$, $\alpha \notin \{0, 1\}$ and $\vec{b} = \vec{0}$. The approximation set for more complex transition relations will be built from these cases.

5.1.1 Case $\alpha = 0$ and $\vec{b} = \vec{0}$..

When $\alpha = 0$, the function $\vec{x} \mapsto N\vec{x}$ is nilpotent. If n is an integer number greater than p then N^n is the zero matrix. The set $\mathbb{Z}$ is not an element of $\mathcal{P}_1(\mathbb{C})$. Therefore the condition *"n is an integer number greater than p"* will be replaced by *"n is a real number greater than p"*.

Proposition 3 *Let $p \geq 1$ be an integer and let $\to$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \to \vec{y} \text{ if and only if } \vec{y} = N\vec{x}$$

where N is a nilpotent p square matrix. The following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\to$:

$$E = \left\{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} \,\middle|\, n \in \{1, \ldots, p-1\} \text{ and } \vec{y} = N^i\vec{x}\right\} \cup \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | n \in \mathbb{R} \text{ and } n \geq p \text{ and } \vec{y} = \vec{0}\}.$$

5.1.2 Case $\alpha = 1$.

For all $n \in \mathbb{N}$, we have the equality:

$$\text{post}^n_{\to}(\{\vec{x}\}) = \left\{ \sum_{0 \leq i \leq max(p-1,n)} \binom{n}{i} N^i\vec{x} + \sum_{0 \leq i \leq max(p-1,n-1)} \binom{n}{i+1} N^i\vec{b} \right\}.$$

Our idea is to abstract this formula into a polynomial one. Firstly, we introduce two auxiliary functions. For each positive integer i, $P_i(X)$ is the polynomial defined by:

$$P_i(X) = \frac{1}{(i)!} \prod_{0 \leq k \leq i-1} (X - k).$$

Fixing $p, N, \vec{b}$, the function f is defined by:

$$f : \begin{array}{ccc} \mathbb{R} \times \mathbb{C}^p & \to & \mathbb{C}^p \\ (n, \vec{x}) & \mapsto & \sum_{0 \leq i \leq p-1} P_i(n)N^i\vec{x} + P_{i+1}(n)N^i\vec{b} \end{array}$$

Proposition 4 *Let p be a strictly positive integer and let $\to$ be the transition relation over $\mathbb{C}^p$ such that :*

$$\vec{x} \to \vec{y} \text{ if and only if } \vec{y} = (Id_p + N)\vec{x} + \vec{b}$$

where N is a nilpotent p square matrix and $\vec{b}$ is a p vector. The following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\to$:

$$E = \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | \vec{y} = f(n, \vec{x})\}.$$

5.1.3 Case $\alpha \notin \{0, 1\}$ and $\vec{b} = \vec{0}$.

Three kinds of asymptotic behaviours of $\stackrel{n}{\to}$ are possible when n goes to $+\infty$ according to the value of $|\alpha|$:

- if $0 < |\alpha| < 1$ then $\stackrel{n}{\rightarrow}(\vec{x})$ converges exponentially in n to $\{\vec{0}\}$,
- if $1 < |\alpha|$ then $\stackrel{n}{\rightarrow}(\vec{x})$ diverges in n,
- if $|\alpha| = 1$ then $\stackrel{n}{\rightarrow}(\vec{x})$ diverges polynomially in n.

For each of these cases, we shall propose an approximation set that will tally with the asymptotic behaviour. We use the following binomial like identity:

$$(\alpha Id_p + N)^n \vec{x} = \alpha^n \sum_{0 \leq i \leq max(p-1,n)} \binom{n}{i} \alpha^{-i} N^i \vec{x}.$$

If $\alpha \neq 1$ then the behaviour of α^n cannot be represented as a polynomial in n. Hence, α^n is replaced by a weaker constraint on n whose degree will be chosen according to the asymptotic behaviour. For all $\alpha \notin \{0,1\}$, ϕ_α is the function from $\mathbb{R}$ into $\mathcal{P}_1(\mathbb{C})$ defined by:

- $\phi_{-1}(n) = \{1, -1\}$,
- if $|\alpha| = 1$ and $\alpha \notin \{1, -1\}$ then $\phi_\alpha(n) = \{c \in \mathbb{C} | |c|^2 = 1\}$,
- if $|\alpha| > 1$ then $\phi_\alpha(n) = \{c \in \mathbb{C} | |c|^2 \geq ((|\alpha| - 1) \cdot n + 1)^2\}$,
- if $0 < |\alpha| < 1$ then $\phi_\alpha(n) = \left\{ c \in \mathbb{C} \,\middle|\, |c|^2 \cdot \left((|\alpha|^{-1/p}) - 1 \cdot n + 1 \right)^{2p} \leq 1 \right\}$.

Fixing p, N, α, the function g is defined by:

$$g : \begin{array}{ccc} \mathbb{C} \times \mathbb{C}^p & \rightarrow & \mathbb{C}^p \\ (n, \vec{x}) & \mapsto & \sum_{0 \leq i \leq p-1} P_i(n) \alpha^{-i} N^i \vec{x} \end{array}$$

We can now describe the approximation set.

Proposition 5 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x}$$

where $\alpha \in \mathbb{C} \setminus \{0, 1\}$ and N is a nilpotent p square matrix. The following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E = \{(n, \vec{x}, \vec{y}) \mid \text{ there exists } c \in \mathbb{C} \text{ such that } c \in \phi_\alpha(n) \text{ and } \vec{y} = c \cdot g(n, \vec{x}) \}.$$

Remark 2 *We can evaluate these approximation sets by a qualitative analysis of their asymptotic behaviour. Let us show that the approximated transition relation $E(n)$ has a similar asymptotic behaviour as $\stackrel{n}{\rightarrow}$. We fix a vector and we compare the states that can be reached using $\rightarrow$ and the approximated transition relation. The variable n is an integer and we study the approximated transition relation when n goes to $+\infty$:*

(a) if $\alpha = -1$ then for all $\vec{x}$, for all positive integer $n \geq 1$, $E(n, \vec{x}) = \text{post}^n_\rightarrow(\vec{x}) \cup \{\vec{y} \in \mathbb{C}^p | -\vec{y} \in \text{post}^n_\rightarrow(\{\vec{x}\})\}$;

(b) if $|\alpha| = 1$ and $\alpha \notin \{1, -1\}$ then for all $\vec{x}$, for all positive integer $n \geq 1$, $E(n, \vec{x}) = \{c \cdot \vec{y} | c \in \mathbb{C}$ and $|c| = 1$ and $\vec{y} \in \text{post}^n_\rightarrow(\{\vec{x}\})$;

(c) if $\alpha \in \mathbb{C}^*$ then for all states $\vec{x}$,

$$\lim_{n \to +\infty} \{|\vec{y}| | \vec{y} \in E(n, \vec{x})\} = \lim_{n \to +\infty} \{|\vec{y}| | \vec{y} \in \text{post}^n_\rightarrow(\{\vec{x}\})\}.$$

5.2 Reductions

We first reduce the affine case to the homogeneous case. The case $\alpha \notin \{0,1\}$ and $\vec{b} \neq \vec{0}$ can be reduced to the case $\alpha \notin \{0,1\}$ and $\vec{b} = \vec{0}$ using the following remark. The equality $\vec{y} = (\alpha Id_p + N)\vec{x} + \vec{b}$ is equivalent to $\vec{y} + ((\alpha-1)Id_p + N)^{-1}\vec{b} = (\alpha Id_p + N)(\vec{x} + ((\alpha-1)Id_p + N)^{-1}\vec{b})$. We only need to make a translation of vector $-((\alpha-1)Id_p + N)^{-1}\vec{b}$ to reduce the computation to the previous case.

Proposition 6 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation defined by:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x} + \vec{b}$$

where $\alpha \in \mathbb{C} \setminus \{0\}$, N is a nilpotent p square matrix, $\vec{b}$ is a p vector and let $\rightsquigarrow$ be the transition relation defined by:

$$\vec{x} \rightsquigarrow \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x}.$$

If the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightsquigarrow$ then the following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E' = \{(n, \vec{x}', \vec{y}') \in \mathcal{P}_{2p+1}(\mathbb{C}) | \text{ there exists } (n, \vec{x}, \vec{y}) \in E \text{ such that } \vec{x}' = \vec{x} - ((\alpha-1)Id_p + N)^{-1}\vec{b} \text{ and } \vec{y}' = \vec{y} - ((\alpha-1)Id_p + N)^{-1}\vec{b})\}.$$

We now consider the more general case when the matrix A is a block diagonal matrix with blocks of the form $\alpha Id_p + N$. Our idea is to chose as approximation set the product of the approximation sets in each characteristic space. Note that the variable n allows one to synchronize the approximation sets instead of simply computing the product of the transition relations.

Proposition 7 *Let $p_1, \ldots, p_q$ be strictly positive integers, let $\rightarrow_1, \ldots, \rightarrow_q$ be transition relations such that $\rightarrow_i$ is a transition relation over $\mathbb{C}^{p_i}$, and let $E_1, \ldots, E_q$ be sets such that each E_i is a set of $\mathcal{P}_{2p_i+1}(\mathbb{C})$ that is an approximation set for $\rightarrow_i$. If $p = \sum_{1 \leq i \leq q} p_i$ and if $\rightarrow$ is the transition relation over $\mathbb{C}^p$ equal to $\bigotimes_{1 \leq i \leq q} \rightarrow_i$ then the following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:*

$$E = \left\{ (n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} \;\middle|\; (\vec{x}, \vec{y}) \in \bigotimes_{1 \leq i \leq q} E_i(n) \right\}.$$

Using Theorem 1, we can find a basis in which the matrix A is in Jordan normal form.

Proposition 8 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = A\vec{x} + \vec{b}$$

where A is a p square matrix and $\vec{b}$ a p vector. Let P and B be p square matrices such that B is in form of Jordan and P is reversible and $A = P^{-1}BP$. Let $\rightsquigarrow$ be the transition relation over $\mathbb{C}^p$ such that:

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = B\vec{x} + P\vec{b}.$$

If the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightsquigarrow$ then the following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E' = \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | (n, P\vec{x}, P\vec{y}) \in E\}.$$

Let us consider now the case where the transition relation $\rightarrow$ has a guard, i.e. is of the form:

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{x} \in C \text{ and } \vec{y} = A\vec{x} + \vec{b}$$

et let $\rightsquigarrow$ be the transition relation without guard:

$$\vec{x} \to \vec{y} \text{ if and only if } \vec{y} = A\vec{x} + \vec{b}.$$

For all vector $\vec{x}$ and for all integer n, the state $\vec{y}$ is in the set $\text{post}^n_{\to}(\{x\})$ if there exists a trajectory $\vec{x} = \vec{q_0} \rightsquigarrow \vec{q_1} \rightsquigarrow \ldots \rightsquigarrow \vec{q_{n-1}} \rightsquigarrow \vec{q_n} = \vec{y}$ verifying for all $i \in \{0, \ldots, n-1\}$ the condition $\vec{q_i} \in C$. In this case, $\text{post}^n_{\to}(\{\vec{x}\})$ has exactly one element therefore $\vec{y} \in \text{post}^n_{\to}(\{\vec{x}\})$ is equivalent to

$$\text{for all } i \in \{0, \ldots, n-1\}, \text{post}^i_{\rightsquigarrow}(\{\vec{x}\}) \subseteq C \text{ and } \vec{y} \in \text{post}^n_{\rightsquigarrow}(\{\vec{x}\}).$$

As we did before, we could replace the constraint "$i \in \mathbb{N}$" by "$i \in \mathbb{R}$ and $i \geq 0$" but the real constraint is stronger that the integer one, therefore we would get an under-approximation instead of an upper-approximation. For handling this case we propose two heuristics to build approximations sets and we propose a safe method in case of failure of these heuristics.

Heuristic 1 *Let p be a strictly positive integer and let $\to$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \to \vec{y} \text{ if and only if } \vec{x} \in C \text{ and } \vec{y} = A\vec{x} + \vec{b}$$

where A is a p square matrix, $\vec{b}$ is a p vector and C a set of $\mathcal{P}_p(\mathbb{C})$. Let $\rightsquigarrow$ be the transition relation over $\mathbb{C}^p$ such that:

$$\vec{x} \rightsquigarrow \vec{y} \text{ if and only if } \vec{y} = A\vec{x} + \vec{b}$$

and let the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ be an approximation set for $\rightsquigarrow$. The two following sets E_1 and E_2 of $\mathcal{P}_{2p+1}(\mathbb{C})$ are candidate as approximation sets for $\to$:

$$\begin{aligned} E_1 = \{(n, \vec{x}, \vec{y}) |\ & \text{for all } i \in \mathbb{R},\ 0 \leq i \leq n-1 \text{ implies } \text{post}_{E(i)}(\{\vec{x}\}) \subseteq C \\ & \text{and } \vec{y} \in \text{post}_{E(n)}(\{\vec{x}\})\}, \\ E_2 = \{(n, \vec{x}, \vec{y}) |\ & \text{for all } i \in \mathbb{R},\ 0 \leq i \leq n-1 \text{ implies } E(i, \vec{x}) \cap C \neq \emptyset \\ & \text{and } \vec{y} \in E(n, \vec{x})\}. \end{aligned}$$

If none of the sets E_1 and E_2 is an approximation set (e.g. the closure property may not be verified), then we can construct a safe approximation set that will be less precise (but still useful).

Proposition 9 *Let p be a strictly positive integer and let $\to$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \to \vec{y} \text{ if and only if } \vec{x} \in C \text{ and } \vec{y} = A\vec{x} + \vec{b}$$

where A is a p square matrix, $\vec{b}$ is a p vector and C is a set of $\mathcal{P}_p(\mathbb{C})$. Let $\rightsquigarrow$ be the transition relation over $\mathbb{C}^p$ such that:

$$\vec{x} \rightsquigarrow \vec{y} \text{ if and only if } \vec{y} = A\vec{x} + \vec{b}.$$

If the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightsquigarrow$ then following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\to$:

$$\begin{aligned} E' = \{(1, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | \vec{x} \to \vec{y}\} \cup \\ \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | n \geq 2 \text{ and } \vec{x} \in (E(n-1) \circ \to)(\vec{y})\}. \end{aligned}$$

Let us consider the case of a transition relation $\to$ with guard and input, i.e. of the form:

$$\vec{x} \to \vec{y} \text{ if and only if there exists } \vec{z} \text{ such that } (\vec{x}, \vec{z}) \in C \text{ and } \vec{y} = A\vec{x} + \vec{b} + A'\vec{z}$$

where A and A' are two p square matrices, $\vec{b}$ is a p vector and C is a set of $\mathcal{P}_p(\mathbb{C})$. The transition relation $\to$ may be seen as the union of the transition relations $\to_{\vec{z}}$ where $\vec{z}$ is any vector:

$$\vec{x} \to_{\vec{z}} \vec{y} \text{ if and only if } (\vec{x}, \vec{z}) \in C \text{ and } \vec{y} = A\vec{x} + \vec{b} + A'\vec{z}.$$

There is not general solution to this problem. That is why we propose as a heuristic to compute an approximation set for each $\to_{\vec{z}}$ and to chose the union of these sets as an approximation set for $\to$.

Heuristic 2 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if there exists } \vec{z} \text{ such that } (\vec{x}, \vec{z}) \in C \text{ and } \vec{y} = A\vec{x} + \vec{b} + A'\vec{z}$$

where A and A' are p square matrices, $\vec{b}$ is a p vector and C is a set of $\mathcal{P}_p(\mathbb{C})$. Let $\rightsquigarrow$ be the transition relation over $\mathbb{C}^{2p}$ such that:

$$(\vec{x}, \vec{x'}) \rightsquigarrow (\vec{y}, \vec{y'}) \text{ if and only if } (\vec{x}, \vec{x'}) \in C \text{ and } \vec{y} = A\vec{x} + A'\vec{x'} + \vec{b} \text{ and } \vec{y'} = \vec{x'}.$$

Let E be a set of $\mathcal{P}_{4p+1}(\mathbb{C})$ that is an approximation set for $\rightsquigarrow$. The following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is a candidate for an approximation set for $\rightarrow$:

$$E' = \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | \text{ there exists } \vec{x'}, \vec{y'} \text{ such that } (n, (\vec{x}, \vec{x'}), (\vec{y}, \vec{y'})) \in E\}.$$

5.3 Application to the backward strategy

The previous approach can also be applied directly to backward strategies.

Proposition 10 *Let Q be a set, let $\rightarrow$ be a transition relation over Q and let $\leftarrow$ be the transition relation over Q such that $x \leftarrow y$ is equivalent to $y \rightarrow x$. If the set E is an approximation set for $\rightarrow$ then the following set E' is an approximation set for $\leftarrow$:*

$$E' = \{(n, x, y) | (n, y, x) \in E\}.$$

6 Example

We consider Example 2 again. Let us apply our technique to the transition relations $\rightarrow_1$ and $\rightarrow_3$. The relation $\rightarrow_1$ can be represented as follows:

$$\text{there exists } vp \text{ such that } (v,d) \in \{(x,y) \in \mathbb{R}^2 | vp \geq 0 \text{ and } y - x + amax < 0 \text{ and } x - afu \geq 0\} \text{ and } \begin{bmatrix} v' \\ d' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} v \\ d \end{bmatrix} + \begin{bmatrix} -afu \\ vp + afu \end{bmatrix}.$$

Let $\rightsquigarrow_1$ be the transition relation such that $(v,d) \rightsquigarrow_1 (v',d')$ if and only if $\binom{v'}{d'} = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right) \binom{v}{d} + \binom{-afu}{vp+afu}$. The corresponding approximation set is:

$$\left\{(n, v, d, v', d') \in \mathbb{R}^5 | \binom{v'}{d'} = \left(\begin{smallmatrix} 1 & 0 \\ -n & 1 \end{smallmatrix}\right) \binom{v}{d} + \left(\begin{smallmatrix} n & 0 \\ -\frac{n \cdots (n-1)}{2} & n \end{smallmatrix}\right) \binom{-afu}{vp+afu}\right\}.$$

Then the approximation set for $\rightarrow_1$ is:

$$\{(n, v, d, v', d') \in \mathbb{R}^5 | \text{ there exists } vp \text{ such that } (v,d) \rightarrow (v',d')\} \cup \{(n, v, d, v', d') \in \mathbb{R}^5 | n \geq 2 \text{ and there exists } vp \text{ such that } \binom{v'}{d'} = \left(\begin{smallmatrix} 1 & 0 \\ -n & 1 \end{smallmatrix}\right) \binom{v}{d} + \left(\begin{smallmatrix} n & 0 \\ -\frac{n \cdots (n-1)}{2} & n \end{smallmatrix}\right) \binom{-afu}{vp+afu}\}.$$

A similar computation can be done with $\rightarrow_3$. Then applying the backward reachability algorithm, we get the set of states:

$$\{(v,d) \in \mathbb{R}^2 | v + amax + afu \geq 0 \vee d - v + amax < 0\} \cup \{(v,d) \in \mathbb{R}^2 | d \leq 0\}.$$

No initial state belongs to this set hence the controller is correct. The computation is represented by the tree in Figure 3. Let us note that, compared to the other approaches, our approximation has lead to a better (i.e. smaller) superset of the set of the states that may reach a failure state. Moreover, our technique can be completely automatized whereas in the other approaches the approximation set has to be guessed.

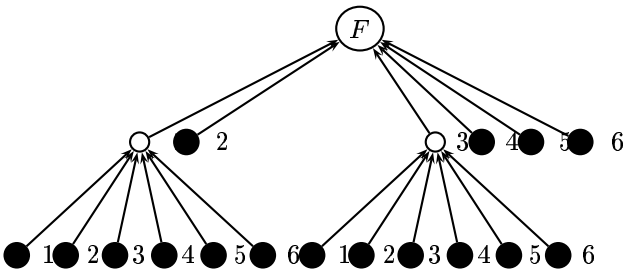

Figure 3: Proof tree for the abstract train controller

7 Conclusion

We have proposed a new technique for constructing metatransitions for real linear transition relations. Our approach takes into consideration the asymptotic behaviour of the system which depends of its eigenvalues and the dimension of the associated characteristic spaces. Compared to previous work, we improve the class of transition relations for which we can construct a metatransition. Finally, we use polynomials to represent these metatransitions.

We plan to improve this work in two directions. Firstly, using a similar approach, we can construct linear metatransitions that would be easier to manipulate but may produce less precise approximations. Secondly, we should be able to handle also linear differential systems: The solution of the differential equation $\dot{\vec{x}}(t) = A\vec{x}(t)$ is $\vec{x}(t) = \vec{x}(0) \cdot exp(At)$. We conjecture that the metatransition $\rightsquigarrow$ associated to the transition relation $\vec{x} \rightarrow exp(A)\vec{x}$ verifies $\vec{x}(t) \rightsquigarrow \vec{x}(0) \cdot exp(At)$. Hence our approach should apply directly to continuous transitions relations as the ones used in hybrid automaton.

References

[1] S. Bensalem, P. Caspi, C. Parent-Vigouroux, and C. Dumas. A methodology for proving control systems with Lustre and PVS. In Charles B. Weinstock and John Rushby, editors, *Dependable Computing for Critical Applications—7*, volume 12 of *Dependable Computing and Fault Tolerant Systems*, pages 89–107, San Jose, CA, January 1999. IEEE Computer Society Press.

[2] S. Bensalem, Y. Lakhnech, and S. Owre. Computing abstractions of infinite state systems compositionally and automatically. In *Proc. 10th International Computer Aided Verification Conference*, pages 319–331, 1998.

[3] A. Benveniste and P. LeGuernic. Hybrid dynamical systems theory and the SIGNAL language. *IEEE Transactions on Automatic Control*, 35(5):535–546, May 1990.

[4] B. Boigelot. *Symbolic Methods for Exploring Infinite State Spaces.* PhD thesis, Université de Liège, 1998.

[5] P. Caspi, D. Pilaud, N. Halbwachs, and J. A. Plaice. LUSTRE : A declarative language for programming synchronous systems. In *Proceedings of the 14th ACM Symposium on Principles of Programming Languages*, New York, NY, 1987. ACM.

[6] Edmund M. Clarke, Orna Grumberg, and Doron A. Peled. *Model Checking.* The MIT Press, Cambridge, Massachusetts, 1999.

[7] P Cousot and R Cousot. Comparing the Galois Connection and Widening/Narrowing Approaches to Abstract Interpretation. In *PLILP'92*, volume 631 of *LNCS*, pages 269–295. Springer-Verlag, 1992.

[8] G. Delzanno and A. Podelski. Model checking in CLP. *Lecture Notes in Computer Science*, 1579:223–239, 1999.

[9] C. Dumas. *Méthodes déductives pour la preuve de programmes LUSTRE.* PhD thesis, Université Joseph Fourier - Grenoble 1, 2002.

[10] E. Allen Emerson. Temporal and modal logic. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics*, pages 995–1072. Elsevier Science Publishers, Amsterdam, The Netherlands, 1990.

[11] A. Finkel and J. Leroux. How to compose Presburger-accelerations: Applications to broadcast protocols. In Proc. 22nd Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS'2002), Kanpur, India, Dec. 2002, volume 2556 of Lecture Notes in Computer Science, pages 145-156. Springer, 2002.

[12] N. Halbwachs. *Synchronous Programming of Reactive Systems.* Kluwer Academic Press, Netherlands, 1993.

[13] N. Halbwachs, F. Lagnier, and P. Raymond. Synchronous observers and the verification of reactive systems. In Netherlands Univ. Twente; Enschede, editor, *Proceedings of Third International Conference on Algebraic Methodology and Software Technology, AMAST*, pages 131–44, 1993.

[14] Thomas A. Henzinger. The theory of hybrid automata. In *Proceedings, 11$^{\text{th}}$ Annual IEEE Symposium on Logic in Computer Science*, pages 278–292, New Brunswick, New Jersey, 27–30 July 1996. IEEE Computer Society Press.

[15] Thomas A. Henzinger and Vlad Rusu Reachability verification for hybrid automata. EECS Department, University of California, Hybrid Systems: Computation and Control (First International Workshop, HSCC'1998)

[16] Andrew Ireland and Alan Bundy. Extensions to a generalization critic for inductive proof. In M. A. McRobbie and J. K. Slaney, editors, *Proceedings of the Thirteenth International Conference on Automated Deduction (CADE-96)*, volume 1104 of *LNAI*, pages 47–61, Berlin, July 30–August 3 1996. Springer.

[17] Monika Maidl. A unifying model checking approach for safety properties of parameterized systems. In *CAV 2001*, volume 2102 of *LNCS*, pages 311–323, 2001.

[18] J.-P. P. Queille and Joseph Sifakis. Fairness and related properties in transition systems: a temporal logic to deal with fairness. *Acta Informatica*, 19(3):195–220, July 1983.

[19] Alexander Schrijver. *Theory of Linear and Integer Programming.* John Wiley and Sons, New York, 1987.

[20] A. Tiwari. Approximate reachability for linear systems. In O. Maler and A. Pnuelu, editors, *Hybrid Systems: Computation and Control HSCC.*

8 Appendix

Proposition 1 *Let $(Q, \rightarrow, I, F)$ be an instance of the safety problem, let Q' and I' be two sets such that $Q \subseteq Q'$, $I \subseteq I' \subseteq Q'$ and $(I' \setminus I) \cap Q = \emptyset$, let $\rightsquigarrow$ be a binary relation over Q' such that $\rightarrow \subseteq \rightsquigarrow$ and for all $x \in Q$, $y \rightsquigarrow x$ implies $y \in Q$ and $y \rightarrow x$. Therefore the two instances $(Q, \rightarrow, I, F)$ and $(Q', \rightsquigarrow, I', F)$ of the safety problem have the same output.*

Proof. Let $q_0 \rightarrow \ldots \rightarrow q_n$ a trajectory of the transition system $(Q, \rightarrow, I)$ such that $q_n \in F$. As $I \subseteq I'$ and $\rightarrow \subseteq \rightsquigarrow$, this trajectory is also a trajectory of $(Q', \rightsquigarrow, I')$ therefore if the answer to $(Q, \rightarrow, I, F)$ is **yes** then the answer to $(Q', \rightsquigarrow, I', F)$ is also **yes**.

Let $q_0 \rightsquigarrow \ldots \rightsquigarrow q_n$ a trajectory of the transition system $(Q, \rightsquigarrow, I')$ such that $q_n \in F$. As $q_n \in Q$, we have $q_{n-1} \in Q$ and by induction for all $i \in \{0, \ldots, n-1\}$, $q_i \in Q$ and $q_i \rightarrow q_{i+1}$. Moreover $q_0 \in Q \cap I$ that is equal to I. We have proven that $q_0 \rightarrow \ldots \rightarrow q_n$ is also a trajectory of $(Q, \rightarrow, I)$. Therefore if the answer to $(Q', \rightsquigarrow, I', F)$ is **yes** then the answer to $(Q, \rightarrow, I, F)$ is also **yes**. □

Proposition 2 *Let $\rightarrow$ be a transition relation over $Q \subseteq \mathbb{C}^p$, and let E be a set of $\mathcal{P}_{2p+1}(\mathbb{C})$ such that $E(1)$ contains $\rightarrow$ and for all integer numbers m and n greater than 1, $E(m) \circ E(n) \subseteq E(m+n)$. Then $\bigcup_{n \in \mathbb{R}, n \geq 1} E(n)$ contains $\rightarrow$ and is closed.*

Proof. The transition relation $\bigcup_{n \in \mathbb{R}, n \geq 1} E(n)$ is denoted by $\rightsquigarrow$. The hypothesis implies that $\rightarrow \subseteq E(1) \subseteq \rightsquigarrow$.

Let us assume that $x \rightsquigarrow y \rightsquigarrow z$; we want to prove that $x \rightsquigarrow z$. The way we have constructed $\rightsquigarrow$ implies that there exists two real numbers m and n,$m \geq 1, n \geq 1$ such that $xE(m)yE(n)z$. Consequently $xE(m+n)z$ and $x \rightsquigarrow z$. We have proven that $\rightsquigarrow \circ \rightsquigarrow \subseteq \rightsquigarrow$. □

Proposition 3 *Let $p \geq 1$ be an integer and let $\rightarrow$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = N\vec{x}$$

where N is a nilpotent p square matrix. The following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E = \left\{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} \,\middle|\, n \in \{1, \ldots, p-1\} \text{ and } \vec{y} = N^i\vec{x}\right\} \cup \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | n \in \mathbb{R} \text{ and } n \geq p \text{ and } \vec{y} = \vec{0}\}.$$

Proof. The binary relation $E(1)$ is $\{(\vec{x}, \vec{y}) \in \mathbb{C}^{2p} | \vec{y} = N\vec{x}\}$ that is equal to $\rightarrow$.

Let $m \geq 1, n \geq 1$ be two real numbers and let us assume that $\vec{x}E(m)\vec{y}E(n)\vec{z}$. There are two sub-cases:

- if $m \in \{1, \ldots, p-1\}$, $n \in \{1, \ldots, p-1\}$ and $m + n < p$ then $\vec{z} = N^{m+n}\vec{x}$ and $\vec{x}E(m+n)N^{m+n}\vec{x}$;
- elsewhere $m + n \geq p$ and $\vec{z} = \vec{0}$ and $\vec{x}E(m+n)\vec{0}$.

We have proven $\vec{x}E(m+n)\vec{z}$. □

Lemma 1 *For all strictly positive integer p, for every nilpotent p square matrix N, for every vector $\vec{x}$, for all real numbers m and n, $f(n, f(m, \vec{x})) = f(m+n, \vec{x})$.*

Proof. For all positive integer n, $f(n, \vec{x}) = (Id_p + N)^n\vec{x}$. Therefore for all positive integers m and n, $f(n, f(m, \vec{x})) = f(m+n, \vec{x})$. For all $i \in \{1, \ldots, p\}$, the polynom $(m, n) \mapsto (f(n, f(m, \vec{x})) - f(m+n, \vec{x}))_i$ has the value 0 if m and n are positive integer numbers hence it is the zero polynom. Consequently, $f(n, f(m, \vec{x})) = f(m+n, \vec{x})$ for all real numbers m and n. □

Lemma 2 *For all $\alpha \in \mathbb{C}^*$, $\alpha \in \phi_\alpha(1)$, and for all real numbers $m \geq 1, n \geq 1$, $c \in \phi_\alpha(m)$ and $c' \in \phi_\alpha(n)$ imply $c \cdot c' \in \phi_\alpha(m+n)$.*

Proof. Cases $|\alpha| = 1$ are obvious because $\phi_\alpha(n)$ does not depend on n. For the two other cases:

- if $|\alpha| > 1$ then $\phi_\alpha(1) = \{c \in \mathbb{C} | |c|^2 \geq |\alpha|^2\}$ therefore $\alpha \in \phi_\alpha(1)$, and if $c \in \phi_\alpha(m)$ and $c' \in \phi_\alpha(n)$ then

$$\begin{aligned} |c \cdot c'|^2 &\geq (((|\alpha| - 1) \cdot m + 1) \cdot ((|\alpha| - 1) \cdot n + 1))^2 \\ &\geq ((|\alpha| - 1)^2 \cdot m \cdot n + (|\alpha| - 1) \cdot (m + n) + 1)^2 \\ &\geq ((|\alpha| - 1) \cdot (m + n) + 1)^2 \end{aligned}$$

  therefore $c \cdot c' \in \phi_\alpha(n + m)$;

- if $0 < |\alpha| < 1$ then $\phi_\alpha(1) = \left\{c \in \mathbb{C} \,\middle|\, |c|^2 |\alpha^{-2}| \leq 1\right\}$ therefore $\alpha \in \phi_\alpha(1)$, and if $c \in \phi_\alpha(m)$ and $c' \in \phi_\alpha(n)$ then we obtain

$$\begin{aligned} |c \cdot c'|^2 \cdot \left(((|\alpha|^{-1/p} - 1) \cdot m + 1) \cdot ((|\alpha|^{-1/p} - 1) \cdot n + 1)\right)^{2p} &\leq 1 \\ |c \cdot c'|^2 \cdot \left((|\alpha|^{-1/p} - 1)^2 \cdot m \cdot n + (|\alpha|^{-1/p} - 1) \cdot (m + n) + 1\right)^{2p} &\leq 1 \\ |c \cdot c'|^2 \cdot \left((|\alpha|^{-1/p} - 1) \cdot (m + n) + 1\right)^{2p} &\leq 1 \end{aligned}$$

  therefore $c \cdot c' \in \phi_\alpha(m + n)$.

□

Proposition 4 *Let p be a strictly positive integer number and let $\rightarrow$ be the transition relation over $\mathbb{C}^p$ such that :*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = (Id_p + N)\vec{x} + \vec{b}$$

where N is a nilpotent p square matrix and $\vec{b}$ is a p vector. The following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E = \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | \vec{y} = f(n, \vec{x})\}.$$

Proof. The set $E(1)$ is $\{(\vec{x}, \vec{y}) \in \mathbb{C}^{2p} | \vec{y} = N\vec{x} + \vec{b}\}$ that is equal to $\rightarrow$.

Let $m \geq 1, n \geq 1$ be two real numbers and let us assume that $\vec{x}E(m)\vec{y}E(n)\vec{z}$. Therefore, $\vec{z} = f(m, f(n, \vec{x})) = f(m + n, \vec{x})$ hence $\vec{x}E(m + n)\vec{z}$. □

Lemma 3 *For all $\alpha \in \mathbb{C}^*$, $\vec{x} \in \mathbb{C}^p$, and for all real numbers $(m, n) \in \mathbb{R}^2$, $g(n, (g(m, \vec{x})) = g(m + n, \vec{x})$.*

Proof. The proof is similar to the proof of Lemma 1. □

Proposition 5 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x}$$

where $\alpha \in \mathbb{C} \setminus \{0, 1\}$ and N is a nilpotent p square matrix. The following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E = \{(n, \vec{x}, \vec{y}) \mid \text{there exists } c \in \mathbb{C} \text{ such that } c \in \phi_\alpha(n) \text{ and } \vec{y} = c \cdot g(n, \vec{x})\}.$$

Proof. For the first condition, we have

$$\begin{aligned} E(1) &= \{(\vec{x}, \vec{y}) \mid \text{there exists } c \in \mathbb{C} \text{ such that } c \in \phi_\alpha(1) \text{ and } \vec{y} = c \cdot g(1, \alpha, \vec{x})\} \\ &\supseteq \{(\vec{x}, \vec{y}) \,|\vec{y} = \alpha \cdot (Id_p + N)\vec{x})\} \supseteq \rightarrow . \end{aligned}$$

Assume that $\vec{x}E(m)\vec{y}E(n)\vec{z}$ then there exists two complex numbers c and c' such that $c \in \phi_\alpha(m)$, $\vec{y} = c \cdot g(m, \vec{x})$, $c' \in \phi_\alpha(n)$ and $\vec{z} = c' \cdot g(n, \vec{y})$. Hence $\vec{z} = c' \cdot g(n, c \cdot g(m, \vec{x}) = c' \cdot c \cdot g(m + n, \vec{x})$. As $c \cdot c' \in \phi_\alpha(m + n)$, we have proven that $\vec{x}E(m + n)\vec{z}$. □

Lemma 4 *Let $\rightsquigarrow$ be a transition relation over a set Q, let h be a bijection from Q into Q and let $\rightarrow$ be the transition relation over Q such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } h(\vec{y}) \rightsquigarrow h(\vec{x}).$$

If E is an approximation set for $\rightsquigarrow$ then the following set E' is an approximation set for for $\rightarrow$:

$$E' = \{(n, \vec{x}, \vec{y}) | (n, h(\vec{x}), h(\vec{y}) \in E\}.$$

Proof. Assume that $\vec{x} \rightarrow \vec{y}$ then $h(\vec{x}) \rightsquigarrow h(\vec{y})$ and $(1, h(\vec{x}), h(\vec{y})) \in E$. Hence $\vec{x} \in E'(1)\vec{y}$.

Let us assume that $\vec{x}E'(m)\vec{y}E'(n)\vec{z}$. Using the definition of E', we get $h(\vec{x})E(m)h(\vec{y})E(n)h(\vec{z})$. Therefore $h(\vec{x})E(m+n)h(\vec{z})$ and $\vec{x}E'(m+n)\vec{z}$. □

Proposition 6 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x} + \vec{b}$$

where $\alpha \in \mathbb{C} \setminus \{0\}$, N is a nilpotent p square matrix, $\vec{b}$ is a p vector and let $\rightsquigarrow$ be the transition relation such that:

$$\vec{x} \rightsquigarrow \vec{y} \text{ if and only if } \vec{y} = (\alpha Id_p + N)\vec{x}.$$

If the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightsquigarrow$ then the following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E' = \{(n, \vec{x}', \vec{y}') \in \mathcal{P}_{2p+1}(\mathbb{C}) | \text{ there exists } (n, \vec{x}, \vec{y}) \in E \text{ such that } \vec{x}' = \vec{x} - ((\alpha-1)Id_p + N)^{-1}\vec{b} \text{ and } \vec{y}' = \vec{y} - ((\alpha-1)Id_p + N)^{-1}\vec{b})\}.$$

Proof. We apply Lemma 4 with $h(\vec{x}) = \vec{x} + ((\alpha-1)Id_p + N)^{-1}\vec{b}$. □

Proposition 7 *Let $p_1, \ldots, p_q$ be strictly positive integers, let $\rightarrow_1, \ldots, \rightarrow_q$ be transition relations such that $\rightarrow_i$ is a transition relation over $\mathbb{C}^{p_i}$, and let $E_1, \ldots, E_q$ be sets such that E_i is a set of $\mathcal{P}_{2p_i+1}(\mathbb{C})$ that is an approximation set for $\rightarrow_i$. If $p = \sum_{1 \leq i \leq q} p_i$ and if $\rightarrow$ is the transition relation over $\mathbb{C}^p$ equal to $\bigotimes_{1 \leq i \leq q} \rightarrow_i$ then the following set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:*

$$E = \left\{ (n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} \,\middle|\, (\vec{x}, \vec{y}) \in \bigotimes_{1 \leq i \leq q} E_i(n) \right\}.$$

Proof. For all $\vec{x} \in \mathbb{C}^p$, there exists $\vec{x_1}, \ldots, \vec{x_q}$ such that for all $i \in \{1, \ldots, q\}$, $\vec{x_i} \in \mathbb{C}^{p_i}$ and $\vec{x} = (\vec{x_1}, \ldots, \vec{x_q})$. Assume that $\vec{x} \rightarrow \vec{y}$ then for all $i \in \{1 \ldots, q\}$, $\vec{x_i} \rightarrow \vec{y_i}$ hence, by hypothesis on E_i, $\vec{x_i}E_i(1)\vec{y_i}$. Therefore, $\vec{x}E(1)\vec{y}$.

Assume that $\vec{x}E(m)\vec{y}E(n)\vec{z}$. Then for all $i \in \{1 \ldots, q\}$, $\vec{x_i}E_i(m)\vec{y_i}E_i(n)\vec{z_i}$. Therefore $\vec{x_i}E_i(m+n)\vec{z_i}$ and $\vec{x}E(m+n)\vec{z}$. □

Proposition 8 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = A\vec{x} + \vec{b}$$

where A is a p square matrix and $\vec{b}$ is a p vector. Let P and B be p square matrices such that B is in form of Jordan and P is reversible and $A = P^{-1}BP$. Let $\rightsquigarrow$ be the transition relation over $\mathbb{C}^p$ such that:

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{y} = B\vec{x} + P\vec{b}.$$

If the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightsquigarrow$ then the following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E' = \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | (n, P\vec{x}, P\vec{y}) \in E\}.$$

Proof. We apply Lemma 4 with $h(\vec{x}) = P\vec{x}$. □

Proposition 9 *Let p be a strictly positive integer and let $\rightarrow$ be the transition relation over $\mathbb{C}^p$ such that:*

$$\vec{x} \rightarrow \vec{y} \text{ if and only if } \vec{x} \in C \text{ and } \vec{y} = A\vec{x} + \vec{b}$$

where A is a p square matrix, $\vec{b}$ is a p vector and C is a set of $\mathcal{P}_p(\mathbb{C})$. Let $\rightsquigarrow$ be the transition relation over $\mathbb{C}^p$ such that:

$$\vec{x} \rightsquigarrow \vec{y} \text{ if and only if } \vec{y} = A\vec{x} + \vec{b}.$$

If the set E of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightsquigarrow$ then following set E' of $\mathcal{P}_{2p+1}(\mathbb{C})$ is an approximation set for $\rightarrow$:

$$E' = \{(1, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | \vec{x} \rightarrow \vec{y}\} \cup \{(n, \vec{x}, \vec{y}) \in \mathbb{C}^{2p+1} | n \geq 2 \text{ and } \vec{x}E(n-1)\circ \rightarrow \vec{y}\}.$$

Proof. We have $E(1) = \rightarrow$.

Let us assume that $\vec{x}E'(m)\vec{y}E'(n)\vec{z}$ then $\vec{x}E(m-1)\circ \rightarrow \circ E(n-1)\circ \rightarrow \vec{z}$ with eventually $E(0)$ equal to the identity relation. We have $\rightarrow \subseteq \rightsquigarrow$ therefore $E(m-1)\circ \rightarrow \circ E(n-1)$ is included in $E(m+n-1)$. Then $\vec{x}E'(m+n)\vec{z}$. □

Proposition 10 *Let Q be a set, let $\rightarrow$ be a transition relation over Q and let $\leftarrow$ the transition relation over Q such that $x \leftarrow y$ is equivalent to $y \rightarrow x$. If the set E is an approximation set for $\rightarrow$ than the following set E' is an approximation set for $\leftarrow$:*

$$E' = \{(n, x, y) | (n, y, x) \in E\}.$$

Proof. We have $\rightarrow \in E(1)$ therefore $\leftarrow \in E'(1)$.

If $xE'(m)yE'(n)z$ then $yE(m)x$ and $zE(n)y$. As E is an approximation set for $\rightarrow$, $zE(m+n)x$ then $xE'(m+n)z$. □

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Futurs : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399