Policy iteration in finite templates domain

Assalé Adjé [1,2]

DTIM
Onera Toulouse
31055 Toulouse Cedex 4 - France.

Abstract

We prove in this paper that policy iteration can be generally defined in finite domain of templates using Lagrange duality. Such policy iteration algorithm converges to a fixed point when for very simple technique condition holds. This fixed point furnishes a safe over-approximation of the set of reachable values taken by the variables of a program. We prove also that policy iteration can be easily initialised for one single loop programs when templates are correctly chosen.

Keywords: Abstract interpretation, policy iteration, convex optimisation.

1 Introduction

We introduced a complete lattice consisting of sub-level sets of (possibly non-convex) functions, which we use as an abstract domain in the sense of abstract interpretation [CC77] for computing numerical program invariants. This abstract domain is parameterised by a basis of functions, akin to the approach put forward by Manna, Sankaranarayanan, and Sipma (the linear template abstract domain [SSM05]), except that the basis functions or templates which we use here need not be linear. The templates can be thought as invariant algebraic relations which help to prove correctness of the programs. Previously, the set of templates have been provided by an user. Natural invariant quadratic relations as Lyapunov functions to discrete linear systems have been considered [AGG10a,AGG11]. More recently, for similar systems, Lyapunov functions certified in floating-point arithmetic have been generated automatically using semi-definite programming [RJGF12].

In this paper, we propose a generalised approach to compute "good" templates in Section 7 and prove that policy iteration for one single loop programs can be easily initialised when templates are correctly chosen. Moreover, we show in Subsection 6.3

[1] Email: `assale.adje@onera.fr`

[2] `The author is supported by the RTRA / STAE Project BRIEFCASE.`

that policy iteration described in [AGG10a,AGG11] actually converges to a fixed point of the relaxed semantics $F^{\mathcal{R}}$ (see Theorem 6.3) whereas previous result only shows that a postfixpoint was approximated.

2 Recalling the generalised templates

In [AGG10b,AGG11], we introduced the concept of generalised templates which are just functions from $\mathbb{R}^d$ to $\mathbb{R}$. We can think of hidden algebraic relations to prove certain properties on the analysed program. We suppose that these functions are given by some oracles. Suppose that the subset of relations between variables is fixed, we denote by $\mathbb{P}$ this set and $\mathbb{P} \subseteq \mathbf{F}\left(\mathbb{R}^d, \mathbb{R}\right)$. First, we recall the basic definitions (abstraction and concretisation maps) and prove that this pair of maps forms a Galois connection. Then we describe the lattice structures of abstract and concrete domains.

2.1 Basic notions

We are interested in replacing the classical concrete semantics by meaning of sub-level sets i.e. we have a functional representation of numerical invariants through the functions of $\mathbb{P}$. An invariant will be determined as the intersection of sub-level sets. The problem is thus reduced to find the optimal levels on each templates p. We introduce a set of functions from $\mathbb{P}$ to $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty\} \cup \{+\infty\}$ denoted by $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$. For an element $v \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$, we associate the intersection of sub-level sets defined by $v(p)$ where p belongs to $\mathbb{P}$.

Definition 2.1 ($\mathbb{P}$-sub-level sets) *To a function $v \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$, we associate the $\mathbb{P}$-sub-level set denoted by $v^\star$ and defined as:*

$$v^\star = \{x \in \mathbb{R}^d \mid p(x) \leq v(p),\ \forall p \in \mathbb{P}\} = \bigcap_{p \in \mathbb{P}} \{x \in \mathbb{R}^d \mid p(x) \leq v(p)\}$$

When $\mathbb{P}$ is a set of convex functions, the $\mathbb{P}$-sub-level sets corresponds to the intersection of classical sub-level sets from convex analysis. In our case, $\mathbb{P}$ can contain non-convex functions so $\mathbb{P}$-sub-level sets are not necessarily convex in the usual sense.

We also want a functional representation of a set. In convex analysis, it is well-known that a closed convex set can be represented by its support function i.e. the supremum of linear forms on the set (e.g see Section 13 of [Roc96]). Here, we use the same notion but we replace the linear forms by the functions $p \in \mathbb{P}$ which are not necessarily linear. This generalisation is not new and was introduced by Moreau [Mor70]. The reader can be also consult [Rub00,Sin97] for more details about those concepts.

Definition 2.2 ($\mathbb{P}$-support functions) *To $X \subseteq \mathbb{R}^d$, we associate the abstract support function denoted by $X^\dagger$ and defined as:*

$$X^\dagger(p) = \sup_{x \in X} p(x)$$

We equip the $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$ with the classical partial order for the functions i.e $v \leq w \iff v(p) \leq w(p)$ for all $p \in P$. We order the set of the subsets of $\mathbb{R}^d$ by the inclusion. By taking these orders, we get the following proposition.

Proposition 2.1 *The pair of maps $v \mapsto v^\star$ and $X \mapsto X^\dagger$ defines a Galois connection between $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$ and the set of subsets of $\mathbb{R}^d$.*

In the terminology of abstract interpretation, $(.)^\dagger$ is the abstraction function, and $(.)^\star$ is the concretisation function. The Galois connection result will provide the correctness of the semantics.

2.2 The lattices of $\mathbb{P}$-convex sets and $\mathbb{P}$-convex functions

Now, we are interested in closed elements (in term of Galois connection) that we call here $\mathbb{P}$-convex elements. Formally, they are defined as follows.

Definition 2.3 ($\mathbb{P}$-convexity) *Let $v \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$, we say that v is a $\mathbb{P}$-convex function if $v = (v^\star)^\dagger$. A set $X \subset \mathbb{R}^d$ is a $\mathbb{P}$-convex set if $X = (X^\dagger)^\star$.*

Definition 2.4 *We respectively denote by $\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})$ and $\mathrm{Vex}_{\mathbb{P}}(\mathbb{R}^d)$ the set of $\mathbb{P}$-convex function of $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$ and the set of $\mathbb{P}$-convex sets of $\mathbb{R}^d$.*

The family of functions $\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})$ is ordered by the partial order of real-valued functions i.e $v \leq w \iff v(p) \leq w(p)\ \forall p \in \mathbb{P}$. The family of set $\mathrm{Vex}_{\mathbb{P}}(\mathbb{R}^d)$ is ordered by the inclusion order denoted by $\subseteq$. Galois connection permits to construct lattice operations on $\mathbb{P}$-convex elements. They are defined as follows.

Definition 2.5 (The meet and join) *Let v and w be in $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)$. We denote by $\inf(v, w)$ and $\sup(v, w)$ the functions defined respectively by, $p \mapsto \inf(v(p), w(p))$ and $p \mapsto \sup(v(p), w(p))$. We equip $\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})$ with the join operator $v \vee w = \sup(v, w)$ and the meet operator $v \wedge w = (\inf(v, w)^\star)^\dagger$. Similarly, we equip $\mathrm{Vex}_{\mathbb{P}}(\mathbb{R}^d)$ with the join operator $X \sqcup Y = ((X \cup Y)^\dagger)^\star$ and the meet operator $X \sqcap Y = X \cap Y$.*

It is well-known that with the previous lattice operations, the lattice sets of $\mathbb{P}$-convex elements are isomorphic complete lattices.

Theorem 2.2 *$(\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}}), \wedge, \vee)$ and $(\mathrm{Vex}_{\mathbb{P}}(\mathbb{R}^d), \sqcap, \sqcup)$ are isomorphic complete lattices.*

3 Abstract semantics

Suppose now we are given a program with d variables $(x_1, \ldots, x_d)$ and n control points numbered from 1 to n. We suppose this program is written in a simple toy version of a `C`-like imperative language, comprising global variables, no procedures, assignments of variables using only *parallel assignments* $(x_1, \ldots, x_d) = T(x_1, \ldots, x_d)$, tests of the form $r(x_1, \ldots, x_d) \leq 0$, where $r : \mathbb{R}^d \mapsto \mathbb{R}^m$ (m denotes the number of conjunctions of real tests), and while loops with similar entry tests. We do not recapitulate the standard collecting semantics that associates to this program a monotone map $F : \left(\wp(\mathbb{R}^d)\right)^n \to \left(\wp(\mathbb{R}^d)\right)^n$ whose least fixed points $\mathrm{lfp}(F)$ has as ith component $(i = 1, \ldots, n)$ the subset of $\mathbb{R}^d$ of values that the d variables $x_1, \ldots, x_d$ can take at control point i. The aim of this section is to compute, inductively on the

syntax, the abstraction (or a good over-approximation of it) $F^\sharp$ of F from $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$ to itself defined as usual as using Proposition 2.1:

$$\begin{array}{rccl} F^\sharp : & \left(\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})\right)^n & \to & \left(\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})\right)^n \\ & v & \mapsto (F(v^\star))^\dagger & := \sup\limits_{y \in F(v^\star))} \mathbf{e}_y \end{array}$$

The notation $v^\star$ is in fact the vector of sets $(v_1^\star, \cdots, v_n^\star)$, $(F(v^\star)^\dagger)$ is also interpreted component-wise and $\mathbf{e}_y$ is the evaluation function (from $\mathbb{P}$ to $\mathbb{R}$) at $y \in \mathbb{R}^d$, $p \mapsto \mathbf{e}_y(p) = p(y)$. We recall that standard collecting semantics F can only take three forms at some breakpoints ℓ.

- For variable assignments with a map $T : \mathbb{R}^d \to \mathbb{R}^d$ which acts on set of breakpoints ℓ': $F_\ell(X) = T(X_{\ell'})$. We will denote by $\mathbb{A}$ the set of breakpoints representing assignments.
- For assignments under tests (for both branches of conditional branchments) with a map $T : \mathbb{R}^d \to \mathbb{R}^d$ (acting on set of breakpoints ℓ') and a test map $r_\ell : \mathbb{R}^d \to \mathbb{R}^m$: $F_\ell(X) = T(X_{\ell'} \cap r_\ell^{-1}(\_))$. We will denote by $\mathbb{I}$ the set of breakpoints representing assignments under tests.
- for unions (for while loops and join of both branches of condition branchments): $F_\ell(X) = X_{\ell_1} \cup X_{\ell_2}$. We will denote by $\mathbb{U}$ the set of breakpoints representing unions.

Finally, the abstract functional $F^\sharp$ takes the following form in case of assignments under tests and assignments (taking $r_\ell \equiv -1$ for instance):

$$F_\ell^\sharp(v) = \begin{cases} \sup\limits_{y \in T\left(v_{\ell'}^\star \cap r_\ell^{-1}(]-\infty, 0])\right)} \mathbf{e}_y = \sup\limits_{\substack{x \in v_{\ell'}^\star \\ r_\ell(x) \leqslant 0}} \mathbf{e}_{T(x)} & \text{if } \ell \in \mathbb{A} \cup \mathbb{I} \\ \sup\limits_{y \in v_{\ell_1}^\star \cup v_{\ell_2}^\star} \mathbf{e}_y = \left(v_{\ell_1}^\star \cup v_{\ell_2}^\star\right)^\dagger & \text{if } \ell \in \mathbb{U} \end{cases} \tag{1}$$

In case of assignments, the abstract functional is the value functional of a constrained optimisation problem and the new least fixed point equation to solve becomes:

$$\inf\{v \in \left(\mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})\right)^n \mid F^\sharp(v) \leqslant v\} \ . \tag{2}$$

4 Relaxed semantics using Lagrange duality

4.1 Lagrange duality

Let f, $\{f_i\}_{i=1,\ldots,k}$ be functions on $\mathbb{R}^d$. Let us consider the following constrained maximisation problem:

$$\sup\{f(x) \mid f_i(x) \leq 0, \, \forall i = 1, \ldots, k\} \tag{3}$$

In constrained optimisation, it is classical to construct another constrained optimisation problem from the initial one in order to solve an easier problem. A

technique called Lagrange duality (for details see for example [AT03, Section 5.3]) consists in adding to the objective function the inner product of the vector of constraints with a positive vector of the euclidean space whose the dimension is the number of constraints. In our context, the value of Problem (3) is given by the following sup-inf (primal) value (4):

$$\sup_{x\in\mathbb{R}^d}\inf_{\lambda\in\mathbb{R}^k_+} f(x)-\sum_{i=1}^{k}\lambda_i f_i(x)\ . \tag{4}$$

A simple result of constrained optimisation called weak duality theorem ensures that if we commute the inf and the sup in Formula (4), the result is greater than the value of Problem (4). The commutation of the inf and the sup gives us the so called (dual) value:

$$\inf_{\lambda\in\mathbb{R}^k_+}\sup_{x\in\mathbb{R}^d} f(x)-\sum_{i=1}^{k}\lambda_i f_i(x)\ . \tag{5}$$

The vectors $\lambda\in\mathbb{R}^k_+$ are called vectors of Lagrange multipliers. The function $\lambda\mapsto\sup_{x\in\mathbb{R}^d} f(x)-\sum_{i=1}^{k}\lambda_i f_i(x)$ is always convex (the image of a segment is smaller than the segment of images) and lower semi-continuous (this notion is recalled at Definition 5.1), so it has good properties to minimise it. If the function $-f$ is convex, if the functions f_i are convex and if the Slater constraint qualification (i.e. there exists $x\in\mathbb{R}^d$ such that $f_i(x)<0$ for all $i=1,\dots,k$) holds then the values of Problem (4) and Problem (5) coincide.

4.2 Abstraction of assignments and test using Lagrange duality

We recall that the abstract functional described at Equation (1) applied to affectations and tests is of the form:

$$F^\sharp_\ell(v)=\sup_{\{x\in\mathbb{R}^d\mid(v_{\ell'}-\mathbf{e}_x)(q)\geq 0,\ \forall q\in\mathbb{P},\ r_\ell(x)\leq 0\}}\mathbf{e}_{T(x)} \tag{6}$$

When we fix a template $p\in\mathbb{P}$, Equation (6) becomes an optimisation problem of the form of Equation (3) and we can use Lagrange duality as in the first step of Subsection 4.1. In our case, Lagrange multipliers are some non-negative functions λ from $\mathbb{P}$ to $\mathbb{R}$. We thus consider the function which we will call the *relaxed* function:

$$F^{\mathcal{R}}_\ell(v):=\inf_{\substack{\lambda\in\mathbf{F}(\mathbb{P},\mathbb{R}_+)\\ \mu\in\mathbb{R}^m_+}}\sup_{x\in\mathbb{R}^d}\mathbf{e}_{T(x)}+\sum_{q\in\mathbb{P}}\lambda(q)\left(v_{\ell'}(q)-q(x)\right)-\mu^\intercal r_\ell(x)\ . \tag{7}$$

When we fix a template $p\in\mathbb{P}$, we have:

$$\left(F^{\mathcal{R}}_\ell(v)\right)(p)=\inf_{\substack{\lambda\in\mathbf{F}(\mathbb{P},\mathbb{R}_+)\\ \mu\in\mathbb{R}^m_+}}\sup_{x\in\mathbb{R}^d}p(T(x))+\sum_{q\in\mathbb{P}}\lambda(q)\left(v_{\ell'}(q)-q(x)\right)-\mu^\intercal r_\ell(x)\ . \tag{8}$$

4.3 Abstraction of loops

Note that the following double inequalities hold for all $v \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$,

$$\sup(\mathrm{vex}_{\mathbb{P}}(v_{\ell_1}), \mathrm{vex}_{\mathbb{P}}(v_{\ell_2})) \leqslant \left(v^\star_{\ell_1} \cup v^\star_{\ell_2}\right)^\dagger \leqslant \sup(v_{\ell_1}, v_{\ell_2}) \tag{9}$$

This means that as for zones, the union of two such $\mathbb{P}$-convex functions v_{ℓ_1} and v_{ℓ_2} is directly given by taking their maximum on each element of the basis of functions $\mathbb{P}$. Nevertheless, during the fixed point iteration (as in Section 6) the functions v_{ℓ_1} and v_{ℓ_2} are not necessarily $\mathbb{P}$-convex. Moreover, if we take the abstract semantics $F^\sharp_\ell(v)$, we do not have an infimum of linear forms (or at least a maximum of linear forms) on the abstract values v_{ℓ_1} and v_{ℓ_2}, a formulation that we need. Finally, we relaxed the abstract semantics $F^\sharp_\ell(v)$ by the supremum itself and:

$$F^{\mathcal{R}}_\ell(v) = \sup(v_{\ell_1}, v_{\ell_2}) \ . \tag{10}$$

5 Properties of the relaxed semantics

The introduction of relaxed semantics aims to get better computational properties of the semantics. We describe in this section the properties of the relaxed semantics which justify the using of the new semantics. In order to reduce the size of the paper, the proofs are skipped.

First, we show at Theorem 5.1 that the computation of an invariant from relaxed semantics will provide a safe over-approximation of the invariant of the abstract semantics.

Theorem 5.1 *Let i be a coordinate in $\mathbb{A} \cup \mathbb{I} \cup \mathbb{U}$. For all $v \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$, $F^\sharp_i(v) \leq F^{\mathcal{R}}_i(v)$.*

Furthermore, we prove monotonicity of the semantics. This property will be crucial to show that policy iteration provides more and more precise over approximation of an invariant until a fixed point is reached.

Proposition 5.2 *For $i \in \mathbb{A} \cup \mathbb{I} \cup \mathbb{U}$, the map $v \mapsto F^{\mathcal{R}}_i(v)$ is monotone on the set $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$.*

Let v be in $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$. We introduce auxiliary functions to make appear some hidden properties. For $i \in \mathbb{A} \cup \mathbb{I}$, we now define, for $p \in \mathbb{P}$, for $(\lambda, \mu) \in \mathbf{F}\left(\mathbb{P}, \mathbb{R}_+\right) \times \mathbb{R}^m_+$, $F^{\lambda,\mu}_i(v)$ by:

$$\left(F^{\lambda,\mu}_i(v)\right)(p) := \sum_{q \in \mathbb{P}} \lambda(q) v_{\ell'}(q) + V^{\lambda,\mu}_i(p) \tag{11}$$

$$\text{where } V^{\lambda,\mu}_i(p) := \sup_{x \in \mathbb{R}^d} p \circ T(x) - \sum_{q \in \mathbb{P}} \lambda(q) q(x) - \mu^\intercal r_\ell(x) \ . \tag{12}$$

The relaxed functional can now be readily rewritten as follows.

Lemma 5.3 *For $i \in \mathbb{A} \cup \mathbb{I}$: $\left(F^{\mathcal{R}}_j(v)\right)(p) = \inf_{\substack{\lambda \in \mathbf{F}(\mathbb{P}, \mathbb{R}_+) \\ \mu \in \mathbb{R}^m_+}} \left(F^{\lambda,\mu}_j(v)\right)(p)$.*

We recall some mathematical tools to get convergence proofs. Some definitions have been earlier given in the text, we give formal definitions here. All topological aspects are understood in the sense of $\mathbb{R}^d$-standard norm topology.

Definition 5.1 (Lower/upper semi-continuous functions) *A function $f : \mathbb{R}^d \mapsto \overline{\mathbb{R}}$ is said to be lower semi-continuous if for all $\alpha \in \mathbb{R}$, the set $\{x \in \mathbb{R}^d \mid f(x) \leq \alpha\}$ is topologically closed. A function $g : \mathbb{R}^d \mapsto \overline{\mathbb{R}}$ is said to be upper semi-continuous if $-g$ is lower semi-continuous.*

A continuous function and (point-wise) supremum of lower semi-continuous functions are lower semi-continuous. Note that f is lower semi-continuous function iff for all $x \in \mathbb{R}^d$ and for all sequence x_n which converges to x that $f(x) \leq \liminf_n f(x_n)$. For a function f lower semi-continuous and order-preserving, we get $f(\sup_n x_n) = g(x) = \sup_n f(x_n)$ for all increasing converging sequence $(x_n)_{n\geq 0}$ to x.

Definition 5.2 (Slater's condition) *Let $f : \mathbb{R}^d \to \mathbb{R}$ and $g : \mathbb{R}^d \mapsto \mathbb{R}^k$. A constrained maximisation $\sup\{f(x) \mid g(x) \leq 0,\ x \in \mathbb{R}^d\}$ satisfies Slater's condition iff there exists $x_0 \in \mathbb{R}^d$ such that $g(x_0) < 0$ i.e. for all coordinates $i = 1, \ldots, k$, $g_i(x_0) < 0$.*

Slater's condition is linked to the non-emptiness of the interior of the set of constraints. Indeed if the interior of set of constraints is nonempty and constraints function g_i are convex and lower-semicontinuous, then $\mathrm{int}(\{x \in \mathbb{R}^d \mid g(x) \leq 0\}) = \{x \in \mathbb{R}^d \mid g(x) < 0\}$, where int denotes the interior set and $g = (g_1, g_2, \ldots, g_m)$.

Depending on templates we choose, it is easy to check Slater's condition. For example, taking a set of templates $\mathbb{P}$ such that $p(0) = 0$ for all $p \in \mathbb{P}$, for $i \in \mathbb{A} \cup \mathbb{I}$, if $v_{\ell(i)}(p) > 0$, then Slater's condition holds for optimisation problem 6 (whenever $r_\ell(x_0) < 0$ is also satisfied for some x_0 such that $v_{\ell'}(p) > p(x_0)$).

Slater's condition is a sufficient condition to the existence of optimal solutions to the minimisation problem which appears in relaxed functional. Indeed Slater's condition implies the level boundiness of the dual functional. Optimal solutions will be used to compute a "pivoting" policy when a fixed point is not reached.

Proposition 5.4 (Selection property) *Let $i \in \mathbb{A} \cup \mathbb{I}$. Assume that the maximisation problem 6 satisfies the Slater's condition and for all $p \in \mathbb{P}$, there exists $(\lambda_p, \mu_p) \in \mathbf{F}(\mathbb{P}, \mathbb{R}_+) \times \mathbb{R}_+^m$ such that:*

$$\sup_{x \in \mathbb{R}^d} \mathbf{e}_{T(x)} - \sum_{q \in \mathbb{P}} \lambda_p(q) q(x) - \mu_p^\intercal r_\ell(x)$$

is finite. Then the minimisation problem 8 admits a solution i.e. for all $p \in \mathbb{P}$, there exists $(\lambda_p{}^*, \mu_p{}^*) \in \mathbf{F}(\mathbb{P}, \mathbb{R}_+) \times \mathbb{R}_+$ such that:

$$\big(F_i^{\mathcal{R}}(v)\big)(p) = p \circ T(x) + \sum_{q \in \mathbb{P}} \lambda_p{}^*(q)\big(v_{\ell'}(q) - q(x)\big) - \mu_p^{*\intercal} r_\ell(x)$$

The last result of this section discuss about continuity of the relaxed functional. Kleene iteration and policy iteration are iterative processes to compute fixed point. It is important to to prove that the limits of the sequences produced by both iterations scheme are fixed point. To show it, we need continuity.

Proposition 5.5 (Continuity result on $F_i^{\mathcal{R}}$) *Let $i \in \mathbb{A} \cup \mathbb{I} \cup \mathbb{U}$. The following assertions holds:*

(i) *Let $p \in \mathbb{P}$. The map from $\mathbf{F}(\mathbb{P}, \mathbb{R})^n$ to $\overline{\mathbb{R}}$, $v \mapsto F_i^{\mathcal{R}}(v)(p)$ is upper semi-continuous.*

(ii) *For all decreasing sequences $(v_n)_{n\geq 0} \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$:*

$$\left(\inf_{n\geq 0} F_i^{\mathcal{R}}(v_n)\right)(p) = \left(F_i^{\mathcal{R}}(\inf_{n\geq 0} v_n)\right)(p) \ .$$

(iii) *Let $p \in \mathbb{P}$. Let $i \in \mathbb{A} \cup \mathbb{I}$. Assume, there exists a nonempty compact set $K_{i,p}$ such that $\left(F_i^{\mathcal{R}}(\cdot)\right)(p) = \inf_{(\lambda,\mu)\in K_{i,p}} F_i^{\lambda,\mu}(\cdot)(p)$; Then:*
   (a) *the map from $\mathbf{F}(\mathbb{P}, \mathbb{R})^n$ to $\overline{\mathbb{R}}$, $v \mapsto F_i^{\mathcal{R}}(v)(p)$ is lower semi-continuous,*
   (b) *for all increasing sequences $(v_n)_{n\geq 0} \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$:*

$$\left(\sup_{n\geq 0} F_i^{\mathcal{R}}(v_n)\right)(p) = \left(F_i^{\mathcal{R}}(\sup_{n\geq 0} v_n)\right)(p) \ .$$

6 Solving fixed point equations

6.1 Fixed point equations in templates domain

We recall that $\mathbb{P}$ is a finite set of templates. The map F is a monotone map which interprets a program with d variables and n labels in $\wp\left(\mathbb{R}^d\right)^n$. We recall that $v^\star$ denotes the vector of sets $((v_1)^\star, \cdots, (v_n)^\star)$ and $F^\sharp(v) = (F(v^\star))^\dagger$ i.e. $\forall\, i$, $F_i^\sharp(v) = (F_i(v^\star))^\dagger$ and $F^{\mathcal{R}}$ is the map, the components of which are the relaxed functions of $F^\sharp$. As usual in abstract interpretation, we are interested in solving the least fixed point equation:

$$\inf\{v \in \mathrm{Vex}_{\mathbb{P}}(\mathbb{P} \mapsto \overline{\mathbb{R}})^n \mid F^\sharp(v) \leq v\} \ . \tag{13}$$

Nevertheless, the function $F^\sharp$ is not easily computable (since the templates p are general). Hence, we solve instead the following fixed point equation in $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$:

$$\inf\{v \in \mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n \mid F^{\mathcal{R}}(v) \leq v\} \ . \tag{14}$$

We next describe and compare two ways of computing (or approximating) the smallest fixed point of the relaxed semantics equation: Kleene iteration in Section 6.2, and policy iteration in Section 6.3.

6.2 Kleene iteration

We denote by $\bot$ the smallest element of $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$ i.e. for all $i = 1, \cdots, n$ and for all $p \in \mathbb{P}$, $\bot_i(p) = -\infty$. The Kleene iteration sequence in $\mathbf{F}\left(\mathbb{P}, \overline{\mathbb{R}}\right)^n$ is thus as follows:

$$v^0 = \bot, \text{ for } k \geq 0, \ v^{k+1} = F^{\mathcal{R}}(v^k) \ .$$

Now using continuity result of Proposition 5.5, we get the following theorem:

Theorem 6.1 *If for all $i \in \mathbb{A} \cup \mathbb{I}$, for all $p \in \mathbb{P}$, there exists a nonempty compact set $K_{i,p}$ such that $\big(F_i^{\mathcal{R}}(\cdot)\big)(p) = \inf_{(\lambda,\mu)\in K_{i,p}} F_i^{\lambda,\mu}(\cdot)(p)$; then Kleene iteration converges to the smallest fixed point of $F^{\mathcal{R}}$.*

Kleene iteration has the inconvenience that the values v^k which are obtained at a given iteration k (before convergence) do not provide a safe invariant. We shall see that policy iteration does not have this inconvenient: even if it is stopped at an intermediate step, it does provide a safe invariant. Moreover, the convergence of the Kleene iteration can be very slow, so it needs to be coupled with an acceleration technique which provides over-approximations. In [AGG10b,AGG11], after a given number of iterations, and during a few iterations, we round bounds outwards with a decreasing precision (akin to the widening used in [GPBG08]).

6.3 Policy Iteration

We present now policy iteration algorithm. As usual, we present first the policies notion and then describe completely policy iteration at Algorithm 1.

6.3.1 Policy definition

A policy iteration algorithm can be used to solve a fixed point equation for a monotone function written as an infimum of a family of simpler monotone functions, obtained by selecting *policies*, see [CGG+05,GGTZ07] for more background. The idea is to solve a sequence of fixed point problems involving simpler functions. In the present setting, we look for a representation of the relaxed function

$$F^{\mathcal{R}} = \inf_{\pi\in\Pi} F^{\pi} \tag{15}$$

where the infimum is taken over a set Π whose elements π are called *policies*, and where each function F^{π} is required to be monotone. The correctness of the algorithm relies on a selection property, meaning in the present setting that for each argument (i, v, p) of the function $F^{\mathcal{R}}$, there must exist a policy π such that $\big(F_i^{\mathcal{R}}(v)\big)(p) = \big(F_i^{\pi}(v)\big)(p)$. The idea of the algorithm is to start from a policy π, compute the smallest fixed point v of F^{π}, evaluate $F^{\mathcal{R}}$ at point v, and, if $v \neq F^{\mathcal{R}}(v)$, determine the new policy using the selection property (see Proposition 5.4) at point v.

Let us now identify the policies. Lemma 5.3 shows that for each template p, each coordinate $F_i^{\mathcal{R}}$ corresponding to an assignment $i \in \mathbb{A} \cup \mathbb{I}$ can be written as the infimum of a family of affine functions $v \mapsto F_i^{\lambda,\mu}(v)$, the infimum being taken over the set of a couple of Lagrange multipliers (λ, μ). Choosing a policy π consists in selecting, for each $i \in \mathbb{A} \cup \mathbb{I}$ and $p \in \mathbb{P}$, a Lagrange multiplier a pair of Lagrange multipliers λ, μ (for $i \in \mathbb{A}$ a Lagrange multiplier has to be chosen, the added test is trivial ans thus μ has to be chosen equal to 0). We denote by $\pi_i(p)$ the value of (λ, μ) chosen by the policy π. Then, the map F^{π} in 15 is obtained by replacing $F_i^{\mathcal{R}}$ by the affine functions appearing in Lemma 5.3, for $i \in \mathbb{A} \cup \mathbb{I}$. For coordinates corresponding to loops, i.e., $i \in \mathbb{U}$, we take $F_i^{\pi} = F_i^{\mathcal{R}}$ (the choice of policy is trivial) since the infimum operation does not appear in the expression of $F^{\mathcal{R}}$ (see Equation 10).

Proposition 5.4 shows that the selection property is valid under a Slater constraint qualification condition. We thus introduce $\mathcal{FS}(P,\overline{\mathbb{R}})^n$, the set of elements of $\mathbf{F}\left(\mathbb{P},\overline{\mathbb{R}}\right)$ which satisfy the Slater condition when the component F_i of F corresponds to an assignment or a test. More concretely: $v \in \mathcal{FS}(P,\overline{\mathbb{R}})^n$, if, for all $i \in \mathbb{A}\cup\mathbb{I}$ the set: $\{x \in \mathbb{R}^d \mid q(x) < v_{\ell'}(q),\ \forall\, q \in \mathbb{P}\} \cap \{x \in \mathbb{R}^d \mid r_\ell(x) < 0\}$ is non-empty.

Note we can do restrictions on policies when degenerate cases appear:

- At some breakpoints i and for corresponding label j, if there exists $p \in \mathbb{P}$ such that $v_j(p) = -\infty$ then we can choose any vector of non-negative λ such that $\lambda(p) \neq 0$. Note that in this case, $F_i^{\mathcal{R}}(v) \equiv -\infty$ and the smallest fixed point of $F^{\mathcal{R}}$ for the coordinate i must check $v_i \equiv -\infty$.
- At some breakpoints i and for corresponding label j, if there exists $p \in \mathbb{P}$ such that $v_j(p) = +\infty$ then we can choose any vector of non-negative λ such that $\lambda(p) = 0$ for all $p \in \mathbb{P}$ such that $v_j(p) = +\infty$.

These two restrictions let us work with finite values when we have to compute optimal policies.

6.4 Algorithm

Algorithm 1 Policy iteration in finite templates domain

1 Choose $\pi^0 \in \Pi$, $k = 0$.

2 Compute $V^{\pi^k} = \{V^{\pi^k}(q)\}_{q\in P}$ and define the associated function F^{π^k} by choosing λ and μ according to policy π^k using Equation 11.

3 Compute the smallest fixed point v^k in $\mathbf{F}\left(\mathbb{P},\overline{\mathbb{R}}\right)^n$ of F^{π^k}.

4 If $w^k \in \mathcal{FS}(P,\overline{\mathbb{R}})^n$ continue otherwise return w^k.

5 Evaluate $F^{\mathcal{R}}(w^k)$, if $F^{\mathcal{R}}(w^k) = w^k$ return w^k otherwise take π^{k+1} s.t. $F^{\mathcal{R}}(w^k) = F^{\pi^{k+1}}(w^k)$. Increment k and go to 2.

In [AGG10b,AGG11], we have proved that policy iteration on quadratic templates converges towards a postfixpoint of our relaxed functional (Theorem 6.2 here). Combined with Theorem 5.1, this postfixpoint is also a postfixpoint of abstract semantics.

Theorem 6.2 *The following assertions hold: (1) $F^{\mathcal{R}}(v^l) \neq v^l \implies F^{\mathcal{R}}(v^l) < v^l$; (2) the sequence v^l computed by Algorithm 1 is strictly decreasing; (3) the limit v^∞ of the sequence v^l is a postfixpoint: $F^{\mathcal{R}}(v^\infty) \leq v^\infty$.*

Theorem 6.2 ensures that Algorithm 1 produces a sequence of safe over-approximations of the numerical invariant we want. Now we complete Theorem 6.2 by showing that actually, Algorithm 1 converges to a fixed point.

Theorem 6.3 (Convergence of Algorithm 1) *If Slater condition is always satisfied then policy iteration converges to a fixed point.*

Proof. Third point of Theorem 6.2 is $F^{\mathcal{R}}(v^\infty) \leq v^\infty$. Now we have to prove that $v^\infty \leq F^{\mathcal{R}}(v^\infty)$. At third step of Algorithm 1, we compute the smallest fixed point of F^{π^k}. Since we have for all $k \geq 0$, $v^{k+1} \leq v^k$ and by the fact that $F^{\pi^{k+1}}$ is

order-preserving we have: $v^{k+1} = F^{\pi^{k+1}}(v^{k+1}) \leq F^{\pi^{k+1}}(v^k) = F^{\mathcal{R}}(v^k)$. Now by taking the infimum on k, we get $v^\infty = \inf_k v^{k+1} = \inf_k v^k \leq \inf_k F^{\mathcal{R}}(v^k)$ and finally using the commutation of decreasing inf thanks to Proposition 5.5 then $\inf_k F^{\mathcal{R}}(v^k) = F^{\mathcal{R}}(\inf_k v^k) = F^{\mathcal{R}}(v^\infty)$ and we conclude that $v^\infty \leq F^{\mathcal{R}}(v^\infty)$. □

For the third step of Algorithm 1, since $\mathbb{P}$ is finite and using Lemma 5.3, F^{π^l} is monotone and affine $\mathbf{F}(\mathbb{P}, \mathbb{R} \cup \{+\infty\})^n$, we compute the smallest fixed point of F^{π^l} by solving the following linear program see [GGTZ07, Section 4]:

$$\min \sum_{i=1}^{n} \sum_{q \in \mathbb{P}} v^i(q) \text{ s.t. } \left(F_k^{\pi_k^l}(v)\right)(q) \leq v_k(q), \ \forall k = 1, \cdots, n, \ \forall q \in \mathbb{P} \tag{16}$$

7 Templates design and initial policies

The choice of the initial policies is a crucial point for the quality of the fixed point found by policy iteration. For example, if we know that the values of the variables are bounded an unbounded first invariant can be a fixed point and policy iteration stops. The choice depends on the template design algorithm.

The set of reachable values taken by the variables of the analysed program is bounded (in the sense of a $\mathbb{R}^d$-norm) if there exists a function P such that P is level bounded ($\forall \alpha \in \mathbb{R}$, $\{x \in \mathbb{R}^d \mid P(x) \leq \alpha\}$ is bounded) and a sub-level of P is an invariant (i.e. contains all possible values taken by the variables of the analysed program). Nevertheless, finding both invariant function (relation) and invariant level seems to be difficult and in a first time, in template design, we only focus on invariant relations. It means that we are looking for a function such that *all* sub-levels are invariant by program updates (assignments and guarded assignments). We can formulate the problem as follows.

Problem 7.1 *Find a function $P : \mathbb{R}^d \to \mathbb{R}$ such that:*

$$\text{For all } \alpha \in \mathbb{R} \text{ there exists } \beta \in \mathbb{R}_+ \text{ such that } P(x) \leq \alpha \implies \|x\|_2^2 \leq \beta; \tag{17a}$$
$$\text{For all } i \in \mathbb{A} \cup \mathbb{I}, \text{ for all } v_i \in \mathbb{R}, \ r_i(x) \leq 0 \wedge P(x) \leq v_i \implies P(T_i(x)) \leq v_i. \tag{17b}$$

We can formulate Problem 7.1 as a constrained maximisation problem and then using Lagrange duality in order to get a more restrictive but easier to solve problem. A solution can be given when affine or polynomial arithmetic are considered. We introduce Problem 7.2 which only deals with inequalities. The formulation in terms of positivity implies that we could consider relaxations such as sum-of-squares [Par03,Las10] to compute polynomial invariants relations. The main issue to this generalisation is the selection of the right degree of the polynomial solution.

Problem 7.2 *Find $P : \mathbb{R}^d \to \mathbb{R}, \{\gamma_i, i \in \mathbb{I}\}, \gamma_i \in \mathbb{R}_+^m)$ such that:*

$$\forall x \in \mathbb{R}^d, \ P(x) - \|x\|_2^2 \geq 0; \tag{18a}$$
$$\forall i \in \mathbb{A} \cup \mathbb{I}, \ \forall x \in \mathbb{R}^d, \ P(x) - P(T_i(x)) + \gamma_i^\intercal r_i(x) \geq 0; \tag{18b}$$

We get the following result: a solution of the set of inequalities of Problem 7.2 gives a solution to Problem 7.1.

Proposition 7.3 (Problem 7.2 solves Problem 7.1) *The following assertions hold: (1) If P satisfies Equation (18a) then P satisfies Equation (17a); (2) if $(P, \{\gamma_i\}_{i\in\mathbb{A}\cup\mathbb{I}})$ satisfies Equation (18b) then $(P, \{\gamma_i\}_{i\in\mathbb{A}\cup\mathbb{I}})$ satisfies Equation (17b).*

Finally, if $(P, \{\gamma_i\}_{i\in\mathbb{A}\cup\mathbb{I}})$ is a solution to Problem 7.2 then $(P, \{\gamma_i\}_{i\in\mathbb{A}\cup\mathbb{I}})$ is a solution to Problem 7.1.

Note that Proposition 7.3 and Inequations (18b) can be used to compute unbounded algebraic invariant relations between variables. Then these relations can be used as templates and finite bounds on them (to compute the "diameter" of the numerical invariant) can be found by using policy iteration. Here we are interested in proving that set of reachable values are bounded and thus consider the whole set of inequalities included Inequality (18a).

Now, we present the second main result of the paper. Let $(P, \{\gamma_i\}_{i\in\mathbb{A}\cup\mathbb{I}})$ be a solution of Problem 7.2. Using a set of templates $\mathbb{P} = \{P, x_i \mapsto x_i^2\}$. Then policy iteration can be easily initialised (independently of Kleene iteration and widening) for one simple loop program i.e. one loop with one update inside.

Theorem 7.4 (Policy iteration initialisation) *Let us consider a relaxed of the form:*

$$\begin{cases} F_1^{\mathcal{R}}(v) = C^\dagger \\ F_2^{\mathcal{R}}(v) = \sup\{v_1, v_3\} \\ F_3^{\mathcal{R}}(v) = \inf\limits_{\substack{\lambda\in\mathbf{F}(\mathbb{P},\mathbb{R}_+)\\ \mu\in\mathbb{R}_+^m}} \sup\limits_{x\in\mathbb{R}^d} \mathbf{e}_{T(x)} + \sum\limits_{q\in\mathbb{P}} \lambda(q)\left(v_2(q) - q(x)\right) - \mu^\intercal r_3(x) \end{cases},$$

where C is the nonempty set of the initialisation of the variables and $C^\dagger$ denotes the abstraction of C. Let (P, γ_3) a solution to Problem 7.2. Assume that we use the set of templates $\mathbb{P} = \{x \mapsto x_i^2, i = 1, \ldots, d\} \cup \{P\}$. For all $p' \in \mathbb{P}$, Policy iteration can be initialised with the following policy:

$$\pi_3^0(p') = \left(p \mapsto \begin{cases} 0 & \text{if } p \neq P \\ 1 & \text{if } p = P \end{cases}, \gamma_3\right) \tag{19}$$

Moreover, the following polyhedron: $\{v \in \mathbf{F}(\mathbb{P}, \mathbb{R})^3 \mid F^{\pi^0}(v) \leq v\}$ is nonempty and bounded from below and $\mathrm{lfp}(F^{\pi^0})$ has finite coordinates.

Proof. Consider the initial policy π^0 such that π_3 is given by Equation (19), we have: $F_1^{\pi^0}(v) = C^\dagger$, $F_2^{\pi^0}(v) = \sup\{v_1, v_3\}$, $F_3^{\pi^0}(v) = v_2(P) + V_3^{\pi^0}$, with $V_3^{\pi^0} = \sup_{x\in\mathbb{R}^d} \mathbf{e}_{T(x)} - P(x) - \gamma_3^\intercal r_3(x)$. From Inequality (18a), we have for all $p' \in \mathbb{P}$, $p' \neq P$ that $p'(x) \leq \|x\|_2^2 \leq P(x)$ for all $x \in \mathbb{R}^d$ and then $p'(T(x)) \leq \|T(x)\|_2^2 \leq P(T(x))$ for all $x \in \mathbb{R}^d$ also holds. From Inequality (18b), we have $P(T(x)) \leq P(x) + \gamma_3 r_3(x)$ for all $x \in \mathbb{R}^d$. Finally, $V_3^{\pi^0}(p') = \sup_{x\in\mathbb{R}^d} p'(T(x)) - P(x) - \gamma_3 r_3(x) \leq 0$ for all $p' \in \mathbb{P}$. We conclude that the polyhedron: $K^0 = \{v \in \mathbf{F}(\mathbb{P}, \mathbb{R})^3 \mid F^{\pi^0}(v) \leq v\}$ or

```
x = [0,1];
v: = [0,1];
h = 0.01;
while (true) { [2]
  w = v;
  v = v*(1-h)-h*x;
  x = x+h*w; [3] }
```

Fig. 1. Euler integration scheme of a harmonic oscillator

more precisely $K^0 = \{v \in \mathbf{F}(\mathbb{P},\mathbb{R})^3 \mid C^\dagger \leq v_1,\ v_1 \leq v_2,\ v_3 \leq v_2,\ v_2(P) + V_3^{\pi^0}(p') \leq v_3(p'), \forall p' \in \mathbb{P}\}$ is nonempty and bounded from below then the linear program: $\mathrm{Min}\{\sum_{i=1}^{3}\sum_{p\in\mathbb{P}} v_i(p) \mid v \in K^0\}$ has a finite solution. □

Link to Lyapunov inequality for linear discrete dynamical system

Recall that, for a linear discrete dynamical system $x := Ax$, a quadratic function $x \mapsto x^\intercal Lx$, where L is a $d \times d$ symmetric matrix, is called Lyapunov function iff: L is positive definite i.e. $x^\intercal Lx > 0$ for all nonzero $x \in \mathbb{R}^d$ and $L - A^\intercal LA$ is positive definite. Note that L is positive definite is equivalent up to a multiplicative constant to $L - \mathrm{Id}$ is positive ($x^\intercal(L-\mathrm{Id})x \geq 0$ for all $x \in \mathbb{R}^d$).

Suppose there exists only one (convergent) linear update in the analysed program without guards (test is of the form $-1 \leq 0$), then $(x \mapsto x^\intercal Lx, 0)$ is a solution of Problem 7 for every Lyapunov function $x \mapsto x^\intercal Lx$. An algorithm to compute automatically floating points certified Lyapunov functions for while infinite loops and one (guarded) affine update has been developed in [DM12].

8 Examples

8.1 With a Lyapunov function

As to illustrate the interest of the approach, let us consider a harmonic oscillator: $\ddot{x} + c\dot{x} + x = 0$. The program of this example which is given at Figure 1 implements an Euler explicit scheme with a small step $h = 0.01$ and $c = 1$, that is, which simulates the linear system $(x,v)^\intercal = T(x,v)^\intercal$ with $T = \begin{pmatrix} 1 & h \\ -h & 1-h \end{pmatrix}$.

By semi-definite programming, we can compute a Lyapunov function for the linear system $(x,v) :\mapsto (x,v)L(x,v)^\intercal$ defined as: $L = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$. Recall that Lyapunov functions for linear updates are solution of Problem 7.2. We also use the quadratic functions $\underline{x} : (x,v) \mapsto x^2$ and $\underline{v} : (x,v) \mapsto v^2$ which corresponds to interval constraints. We introduce the set of templates $\mathbb{P} = \{\underline{x}, \underline{v}, \underline{L}\}$. The set of templates $\mathbb{P}$ is thus good set of templates in the sense of Section 7 and we can use Theorem 7.4 to initialise Algorithm 1 and so we choose:

$$\pi_3^0(\underline{x}) = (0,0,1),\ \pi_3^0(\underline{v}) = (0,0,1),\ \pi_3^0(\underline{L}) = (0,0,1)\ .$$

In the case of quadratic templates $\mathbb{P}$, it is easy to evaluate functions V^{π}. By semi-definite programming, we find: $V_3^{\pi_3^0}(\underline{x}) = V_3^{\pi_3^0}(\underline{v}) = V_3^{\pi_3^0}(\underline{L}) = 0$. To compute the least fixed point of F^{π^0}, we solve the linear program (see 16), we find:

$$\begin{array}{lll} u_1^0(\underline{x}) = 1.0000 & u_2^0(\underline{x}) = 7.0000 & u_3^0(\underline{x}) = 7.0000 \\ u_1^0(\underline{v}) = 1.0000 & u_2^0(\underline{v}) = 7.0000 & u_3^0(\underline{v}) = 7.0000 \\ u_1^0(\underline{L}) = 7.0000 & u_2^0(\underline{L}) = 7.0000 & u_3^0(\underline{L}) = 7.0000 \end{array}$$

After 5 iterations, policy iteration stops with a fixed point which provides the following numerical invariant at loop:

$$\{x^2 \leq 3.5000,\ v^2 \leq 2.3333,\ 2x^2 + 3v^2 + 2xv \leq 7\}\ .$$

8.2 Unbounded case

We consider a program which contains a loop while and non trivial test. This program is described at Figure 2.

```
i=0;
j=0;[1]
  while [2](i<=42){
      i=i+1;
      j=j+i;[3]
      }
```

Fig. 2. A simple program with a loop and a test

We want to prove that $j \leq \dfrac{i(i+1)}{2}$. We use policy iteration to prove it. The numerical invariant is unbounded and thus for using Proposition 7.3, we can only check whether Inequality (18b) holds to initialise our policy iteration. We are looking for non-negative μ such that:

$$-\frac{(i+1)(i+2)}{2} + j + i + \frac{i(i+1)}{2} - j + \mu(42 - i) \leq 0\ \forall\,(i,j) \in \mathbb{R}^2$$

A simple calculus permits to show that the inequality holds for $\mu = 0$. So we use the singleton set of templates $\mathbb{P} = \{(i,j) \mapsto -\dfrac{i(i+1)}{2} + j\}$. Then we can take as initial policy $\pi^0 = (1,0)$ and we get $V_3^{\pi^0} = 0$ and we have to solve the linear program: $\text{Min}\{v_1 + v_2 + v_3 \mid v_1 \geq 0,\ v_2 \geq v_1,\ v_2 \geq v_3,\ v_3 \geq v_2\}$. We get $v_1 = v_2 = v_3 = 0$ which is a fixed point of $F^{\mathcal{R}}$ and provides the wanted numerical invariants.

9 Conclusion and Future Works

We define policy iteration algorithm in a general setting using a finite domain of templates. and prove that the algorithm converges to a fixed point of the relaxed

semantics. This result allows us to use characterisation tools [AGG14] to check whether the solution found is the smallest one. We also define the problem of computing good templates and prove that initialisation of policy iteration is provided from this choice of invariant relations. Future works should include an automatic method to compute the invariant algebraic relations and automatic way to initialise policy iteration from the relations generated.

References

[AGG10a] A. Adje, S. Gaubert, and E. Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. In *Proceedings of the 19th European Symposium on Programming (ESOP 2010)*, number 6012 in Lecture Notes in Computer Science, pages 23–42. Springer, 2010.

[AGG10b] Assalé Adjé, Stéphane Gaubert, and Eric Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. In Andrew D. Gordon, editor, *ESOP*, volume 6012 of *Lecture Notes in Computer Science*, pages 23–42. Springer, 2010.

[AGG11] Assalé Adjé, Stéphane Gaubert, and Eric Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. *Logical Methods in Computer Science*, 8(1), 2011.

[AGG14] Assalé Adjé, Stéphane Gaubert, and Eric Goubault. Computing the smallest fixed point of order-preserving nonexpansive mappings arising in positive stochastic games and static analysis of programs. *Journal of Mathematical Analysis and Applications*, 410(1):227 – 240, 2014.

[AT03] A. Auslender and M. Teboulle. *Asymptotic Cones and Functions in Optimization and Variational Inequalities*. Springer, 2003.

[CC77] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York, NY.

[CGG+05] A. Costan, S. Gaubert, E. Goubault, M. Martel, and S. Putot. A policy iteration algorithm for computing fixed points in static analysis of programs. In *Proceedings of the 17th International Conference on Computer Aided Verification (CAV'05)*, volume 3576 of *LNCS*, pages 462–475. Springer, 2005.

[DM12] Thao Dang and Ian M. Mitchell, editors. *Hybrid Systems: Computation and Control (part of CPS Week 2012), HSCC'12, Beijing, China, April 17-19, 2012*. ACM, 2012.

[GGTZ07] S. Gaubert, E. Goubault, A. Taly, and S. Zennou. Static analysis by policy iteration on relational domains. In *Proceedings of the Sixteenth European Symposium Of Programming (ESOP'07)*, volume 4421 of *LNCS*, pages 237–252. Springer, 2007.

[GPBG08] E. Goubault, S. Putot, P. Baufreton, and J. Gassino. Static analysis of the accuracy in control systems: Principles and experiments. In Stefan Leue and Pedro Merino, editors, *Formal Methods for Industrial Critical Systems*, volume 4916 of *Lecture Notes in Computer Science*, pages 3–20. Springer Berlin Heidelberg, 2008.

[Las10] J.B. Lasserre. *Moments, positive polynomials and their applications*. Imperial College Press optimization series. Imperial College Press, 2010.

[Mor70] J. J. Moreau. Inf-convultion, sous-additivé, convexité des fonctions numériques. *Journal de Mathématiques Pures et Appliquées*, 49:109–154, 1970.

[Par03] P. Parillo. Semidefinite programming relaxations for semialgebraic problems. *Math. Prog.*, 96(2, series B):293–320, 2003.

[RJGF12] Pierre Roux, Romain Jobredeaux, Pierre-Loïc Garoche, and Eric Feron. A generic ellipsoid abstract domain for linear time invariant systems. In Dang and Mitchell [DM12], pages 105–114.

[Roc96] R.T. Rockafellar. *Convex Analysis*. Princeston University Press, 1996.

[Rub00] A. M. Rubinov. *Abstract Convexity and Global optimization*. Kluwer Academic Publishers, 2000.

[Sin97] I. Singer. *Abstract Convex Analysis*. Wiley-Interscience Publication, 1997.

[SSM05] S. Sankaranarayanan, H. B. Sipma, and Z. Manna. Scalable analysis of linear systems using mathematical programming. In *The Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05)*, volume 3385 of *LNCS*, pages 25–41, January 2005. http://www.metapress.com/link.asp?id=X2G04CAME7MDKD72.