

COUPLING POLICY ITERATION WITH SEMI-DEFINITE RELAXATION TO COMPUTE ACCURATE NUMERICAL INVARIANTS IN STATIC ANALYSIS

ASSALÉ ADJÉ^a, STÉPHANE GAUBERT^b, AND ERIC GOUBAULT^c

^a LSV, CNRS & ENS de Cachan, 61, avenue du Président Wilson, F-94235 Cachan Cedex, France
e-mail address: assale.adje@lsv.ens-cachan.fr

^b INRIA Saclay and CMAP, Ecole Polytechnique, F-91128 Palaiseau Cedex, France
e-mail address: Stephane.gaubert@inria.fr

^c CEA, LIST (MeASI), F-91191 Gif-sur-Yvette Cedex, France
e-mail address: Eric.Goubault@cea.fr

ABSTRACT. We introduce a new domain for finding precise numerical invariants of programs by abstract interpretation. This domain, which consists of sub-level sets of non-linear functions, generalizes the domain of linear templates introduced by Manna, Sankaranarayanan, and Sipma. In the case of quadratic templates, we use Shor’s semi-definite relaxation to derive safe and computable abstractions of semantic functionals, and we show that the abstract fixpoint can be over-approximated by coupling policy iteration and semi-definite programming. We demonstrate the interest of our approach on a series of examples (filters, integration schemes) including a degenerate one (symplectic scheme).

1. INTRODUCTION

We introduce 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 parametrized by a basis of functions, akin to the approach put forward by Manna, Sankaranarayanan, and Sipma (the linear template abstract domain [SSM05] see also [SCSM06]), except that the basis functions or templates which we use here need not be linear. The domains obtained in this way encompass the classical abstract domains of intervals, octagons and linear templates.

1998 ACM Subject Classification: F.3.2.

Key words and phrases: abstract interpretation; policy iteration; convex programming; quadratic programming; semi-definite programming; Lyapunov functions.

^{a,b,c} This work was performed when the first author was with the MeASI team of CEA, LIST and with CMAP, École Polytechnique, being supported by a PhD Fellowship of the Région Île-de-France. This work was also partially supported by the Arpege programme of the French National Agency of Research (ANR), project “ASOPT”, number ANR-08-SEGI-005 and by the Digiteo project DIM08 “PASO” number 3389.

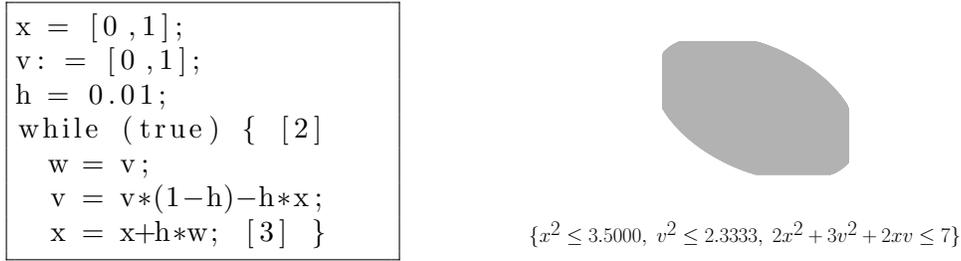


Figure 1: Euler integration scheme of a harmonic oscillator and the loop invariant found at control point 2

To illustrate the interest of this generalization, let us consider a harmonic oscillator: $\ddot{x} + c\dot{x} + x = 0$. By taking an explicit Euler scheme, and for $c = 1$ we get the program shown at the left of Figure 1.

The invariant found with our method is shown right of Figure 1. For this, we have considered the template based on functions $\{x^2, v^2, 2x^2 + 3v^2 + 2xv\}$, i.e. we consider a domain where we are looking for upper bounds of these quantities. This means that we consider the *non-linear* quadratic homogeneous templates based on $\{x^2, v^2\}$, i.e. symmetric intervals for each variable of the program, together with the *non-linear* template $2x^2 + 3v^2 + 2xv$. The last template comes from the Lyapunov function that the designer of the *algorithm* may have considered to prove the stability of his scheme, *before it has been implemented*. This allows us to represent set defined by constraints of the form $x^2 \leq c_1$, $v^2 \leq c_2$ and $2x^2 + 3v^2 + 2xv \leq c_3$ where c_1 , c_2 and c_3 are degrees of freedom. In view of *proving the implementation correct*, one is naturally led to considering such templates¹. Last but not least, it is to be noted that the loop invariant using intervals, zones, octagons or even polyhedra (hence with any linear template) is the insufficiently strong invariant $h = 0.01$ (the variables v and x cannot be bounded.) However, the main interest of the present method is to carry over to the non-linear setting. For instance, we include in our benchmarks a computation of invariants (of the same quality) for an implementation of a highly degenerate example (a symplectic integration scheme, for which alternative methods fail due to the absence of stability margin).

Contributions of the paper. We describe the lattice theoretical operations in terms of Galois connections and generalized convexity in Section 2. We also show that in the case of a basis of quadratic functions, a good over-approximation $F^{\mathcal{R}}$ of the abstraction F^{\sharp} of a semantic functional F can be computed by solving a semi-definite program (Section 3). This over-approximation is obtained using Shor’s relaxation. The advantage of the latter is that it can be solved in polynomial time to an arbitrary prescribed precision by the ellipsoid method [GLS88], or by interior point methods [NN94] if a strictly feasible solution is available (however, we warn the reader that interior points methods, which are more efficient in practice, are known to be polynomial only in the real number model, not in the bit model, see the survey [PR97] for more information).

¹Of course, as for the linear templates of [SSM05, SCSM06], we can be interested in automatically finding or refining the set of templates considered to achieve a good precision of the abstract analysis, but this is outside the scope of this article.

Moreover, we show in Subsection 4.3 that the vectors of Lagrange multipliers produced by this relaxation correspond to policies, in a policy iteration technique for finding fixpoints or at least postfixpoints of $F^{\mathcal{R}}$, precisely over-approximating the fixpoints of F^{\sharp} . Finally, we illustrate on examples (linear recursive filters, numerical integration schemes) that policy iteration on such quadratic templates is efficient and precise in practice, compared with Kleene iteration with widenings/narrowings. The fact that quadratic templates are efficient on such algorithms is generally due to the existence of (quadratic) Lyapunov functions that prove their stability. The method has been implemented as a set of `Matlab` programs.

Related work. This work is to be considered as a generalization of [SSM05], [SCSM06] because it extends the notion of templates to non-linear functions, and of [CGG⁺05], [GGTZ07], [AGG08], [GS07a] and [GS07b] since it also generalizes the use of policy iteration for better and faster resolution of abstract semantic equations. Polynomial inequalities (of bounded degree) were used in [BRCZ05] in the abstract interpretation framework but the method relies on a reduction to linear inequalities (the polyhedra domain), hence is more abstract than our domain. Particular quadratic inequalities (involving two variables - i.e. ellipsoidal methods) were used for order 2 linear recursive filters invariant generation in [Fer05]². Polynomial *equalities* (and not general functional inequalities as we consider here) were considered in [MOS04, RCK07]. The use of optimization techniques and relaxations for program analysis has also been proposed in [Cou05], mostly for synthesising variants for proving termination, but invariant synthesis was also briefly sketched, with different methods than ours (concerning the abstract semantics and the fixpoint algorithm). Finally, the interest of using quadratic invariants and in particular Lyapunov functions for proving control programs correct (mostly in the context of Hoare-like program proofs) has also been advocated recently by E. Féron et al. in [FF08, FA08].

Finally, we note that a preliminary account of the present work appeared in the conference paper [AGG10].

2. LATTICES OF SUB-LEVEL SETS AND P -SUPPORT FUNCTIONS

We introduce a new abstract domain, parametrized by a basis of functions (P below). The idea is that an abstract value will give the bounds for each of these functions, hence the name of sub-level sets, with some abstract convexity condition, Definition 2.9. The abstract values are computed as the supremum of each function of the basis on a certain sub-level set. The name support functions is due to the similarity with the classical support function from convex analysis where the functions of the basis are all linear. The idea of using the classical support function in system verification appeared independently in [LGG09].

2.1. P -sub-level sets, and their Galois connection with $\mathcal{P}(\mathbb{R}^d)$. Let P denote a set of functions from \mathbb{R}^d to \mathbb{R} , which is going to be the basis of our templates. The set P is *not* necessarily *finite* and the functions $p \in P$ are *not* necessarily *linear*. We denote by $\mathcal{F}(P, \overline{\mathbb{R}})$ the set of functions v from P to $\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$. We equip $\mathcal{F}(P, \overline{\mathbb{R}})$ with the classical partial order for functions i.e. $v \leq w \iff v(p) \leq w(p)$ for all $p \in P$. We order the set of all subsets of \mathbb{R}^d by the subset relation \subseteq . We define a Galois connection (Proposition 2.5) between $\mathcal{F}(P, \overline{\mathbb{R}})$ and the set of subsets of \mathbb{R}^d (made of a concretisation

²A generalization to order n linear recursive filters is also sketched in this article.

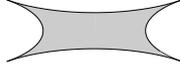
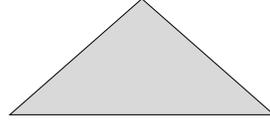


Figure 2: A P -sub-level set arising from non-convex quadratic functions.



$$\{y - x \leq 3, y + x \leq 3, -y \leq 0\}$$

Figure 3: A P -sub-level set arising from linear forms.

operator $v \mapsto v^*$, Definition 2.1 and an abstraction operator $C \mapsto C^\dagger$, Definition 2.4). This will give the formal background for constructing abstract semantics using P -sub-level sets using abstract interpretation [CC77], in Section 3.

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

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

The notion of sub-level set is well known in convex analysis. When P is a set of function that are convex, the P -sub-level sets are convex. In our case, P can contain non-convex functions so P -sub-level sets are not necessarily convex in the classical sense.

Example 2.2. We come back to the first example and we are focusing on its representation in terms of P -sub-level set. Let us write, for $(x, v) \in \mathbb{R}^2$, $p_1 : (x, v) \mapsto x^2$, $p_2 : (x, v) \mapsto v^2$ and $p_3 : (x, v) \mapsto 2x^2 + 3v^2 + 2xv$. Let us take $P = \{p_1, p_2, p_3\}$, $v(p_1) = 3.5000$, $v(p_2) = 2.3333$ and $v(p_3) = 7$. The set v^* is precisely the one shown right of Figure 1.

Example 2.3. We next show some P -sub-level sets which are not convex in the usual sense. Let us write, for $(x, y) \in \mathbb{R}^2$, $p_1 : (x, y) \mapsto -y^2 - (x + 2)^2$, $p_2 : (x, y) \mapsto -y^2 - (x - 2)^2$ and $p_3 : (x, y) \mapsto -(y - 2)^2 - x^2$, $p_4 : (x, y) \mapsto -(y + 2)^2 - x^2$. Let us take $P = \{p_1, p_2, p_3, p_4\}$ and $v(p_1) = v(p_2) = v(p_3) = v(p_4) = -2$. The set v^* is shown Figure 2.

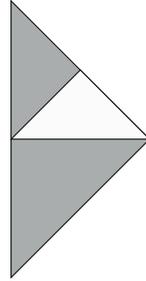
In our case, P is a set of functions from \mathbb{R}^d to \mathbb{R} possibly non-linear, so we generalize the concept of support functions (e.g. see Section 13 of [Roc96]). The idea of generalizing support functions to the non-linear case is not new and this extension is due to Moreau [Mor70].

Definition 2.4 (P -support functions). To $X \subseteq \mathbb{R}^d$, we associate the P -support function denoted by X^\dagger and defined as:

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

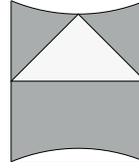
Proposition 2.5. *The pair of maps $v \mapsto v^*$ and $X \mapsto X^\dagger$ defines a Galois connection between $\mathcal{F}(P, \overline{\mathbb{R}})$ and the set of subsets of \mathbb{R}^d .*

Proof. First, the functions $v \mapsto v^*$ and $X \mapsto X^\dagger$ are clearly monotonic. Now, we have to show that, for all $X \subseteq \mathbb{R}^d$ and all $v \in \mathcal{F}(P, \overline{\mathbb{R}})$: $X \subseteq v^* \iff X^\dagger(p) \leq v(p), \forall p \in P$. Let $X \subseteq \mathbb{R}^d$, $v \in \mathcal{F}(P, \overline{\mathbb{R}})$ and $p \in P$. We assume that $X \subseteq v^*$. This implies that $X^\dagger(p) = \sup\{p(x) \mid x \in X\} \leq \sup\{p(x) \mid q(x) \leq v(q), \forall q \in P\}$. But, for every $x \in v^*$, $p(x) \leq v(p)$, so $\sup\{p(x) \mid q(x) \leq v(q), \forall q \in P\} \leq v(p)$, hence, $X^\dagger(p) \leq v(p)$ and the first



$$\{x - y \leq 3, y + x \leq 3, -x \leq 3\}$$

Figure 4: P_1 -convex hull of example 2.8



$$\{y^2 - x^2 \leq 9, x \leq 3, -x \leq 3\}$$

Figure 5: P_2 -convex hull of example 2.8.

implication is shown. Now, we assume that $X^\dagger(p) \leq v(p), \forall p \in P$. Let $x \in X$, we have, for all $p \in P, p(x) \leq X^\dagger(p)$, thus $p(x) \leq v(p)$ and finally $x \in v^*$. \square

Remark 2.6. In the proof, we showed $(v^*)^\dagger \leq v$, we can similarly prove that $X \subseteq (X^\dagger)^*$. Using this remark and using the monotonicity of $v \mapsto v^*$ and $X \mapsto X^\dagger$, we get $v^* \subseteq ((v^*)^\dagger)^* \subseteq v^*$ and similarly, $((X^\dagger)^*)^\dagger = X^\dagger$. These properties are well-known in Galois connection theory.

In the terminology of abstract interpretation, $(.)^\dagger$ is the abstraction function, usually denoted by α , and $(.)^*$ is the concretisation function, usually denoted by γ .

2.2. The lattices of P -convex sets and P -convex functions. The sets of points in \mathbb{R}^d which are exactly represented by their corresponding P -sub-level sets are called P -convex sets, as in the definition below. These can be identified with the set of *abstract elements* we are considering³. We show in Theorem 2.12 that they constitute a complete lattice. We use the terminology P -convex because of the analogy with the abstract convexity defined by Moreau [Mor70], Singer [Sin97] and Rubinov [Rub00]. These authors define convexity without linearity from a given family of (non-linear) functions. Moreau called this notion of convexity, B -convexity where B is the family of functions whereas Singer and Rubinov use the term abstract convexity. The P -convexity defined in this paper corresponds to the classical notions of closure from the Galois connections theory and also to the abstract convexity introduced by Moreau.

Definition 2.7 (P -convex hull). The P -convex hull of an element $v \in \mathcal{F}(P, \overline{\mathbb{R}})$ is the function $\text{vexp}(v)$ which is equal to $(v^*)^\dagger$. Similarly, the P -convex hull of a subset X is the set $\text{vexp}(X)$ which is equal to $(X^\dagger)^*$.

Example 2.8. Let us consider the triangle, depicted in Figure 3. Let us take $P_1 = \{(x, y) \mapsto y + x, (x, y) \mapsto x - y, (x, y) \mapsto -x\}$. Its P_1 -convex hull is the one depicted Figure 4. If we take instead $P_2 = \{(x, y) \mapsto y^2 - x^2, (x, y) \mapsto x, (x, y) \mapsto -x\}$, its P_2 -convex hull is shown in Figure 5.

³Formally, this is the upper-closure in $\mathcal{P}(\mathbb{R}^d)$ of the set of abstract elements.

Definition 2.9 (*P*-convexity). Let $v \in \mathcal{F}(P, \overline{\mathbb{R}})$, we say that v is a *P*-convex function if $v = \text{vexp}(v)$. A set $X \subseteq \mathbb{R}^d$ is a *P*-convex set if $X = \text{vexp}(X)$.

Example 2.10. Let us come back to the triangle depicted in Figure 3. If P is the set of linear forms defined by the faces of this triangle i.e. P consists of the maps $(x, y) \mapsto y - x$, $(x, y) \mapsto y + x$ and $(x, y) \mapsto -y$, then it is a *P*-convex set. But if P is, for example, linear forms defined by orthogonal vectors to the faces of the triangle, the previous triangle is no longer an *P*-convex set.

Abstract (*P*-) convexity is a special instance of Galois connection. The latter are classically used in abstract interpretation. In particular, the theory of Galois connections yields the following result: the *P*-convex hull of a function $v \in \mathcal{F}(P, \overline{\mathbb{R}})$ is the greatest *P*-convex function which is smaller than v and dually the *P*-convex hull of a subset X is the smallest *P*-convex set which is greater than X .

We respectively denote by $\text{Vexp}(P \mapsto \overline{\mathbb{R}})$ and $\text{Vexp}(\mathbb{R}^d)$ the set of all *P*-convex function of $\mathcal{F}(P, \overline{\mathbb{R}})$ and the set of all *P*-convex sets of \mathbb{R}^d .

Definition 2.11 (The meet and join). Let v and w be in $\mathcal{F}(P, \overline{\mathbb{R}})$. We denote by $\inf(v, w)$ and $\sup(v, w)$ the functions defined respectively by:

$$p \mapsto \inf(v(p), w(p)) \text{ and } p \mapsto \sup(v(p), w(p)) .$$

We equip $\text{Vexp}(P \mapsto \overline{\mathbb{R}})$ with the meet (respectively join) operator:

$$v \vee w = \sup(v, w) \tag{2.1}$$

$$v \wedge w = (\inf(v, w))^{\dagger} \tag{2.2}$$

Similarly, we equip $\text{Vexp}(\mathbb{R}^d)$ with the two following operators: $X \sqcup Y = ((X \cup Y)^{\dagger})^{\star}$, $X \sqcap Y = X \cap Y$.

The family of functions $\text{Vexp}(P \mapsto \overline{\mathbb{R}})$ is ordered by the partial order of real-valued functions i.e. $v \leq w \iff v(p) \leq w(p) \forall p \in P$. The family of set $\text{Vexp}(\mathbb{R}^d)$ is ordered by the subset relation denoted by \subseteq . The next theorem follows readily from the fact that the pair of functions $v \mapsto v^{\star}$ and $X \mapsto X^{\dagger}$ defines a Galois connection, see e.g. [DP02, § 7.27].

Theorem 2.12. $(\text{Vexp}(P \mapsto \overline{\mathbb{R}}), \wedge, \vee)$ and $(\text{Vexp}(\mathbb{R}^d), \sqcap, \sqcup)$ are isomorphic complete lattices. \square

2.3. Intervals, Zones, Octagons and Sankaranarayanan et al.'s linear templates.

The domain of intervals arises as a special domain of *P*-convex sets, in which the basis is $P = \{x_1, -x_1, \dots, x_n, -x_n\}$ where x_i ($i = 1, \dots, n$) are the program variables. An abstract value v in our domain encodes the supremum $v(x_i)$ and the infimum $-v(-x_i)$ of an interval for the variable x_i .

Zones and octagons are treated in a similar manner. For instance, for zones, take $P = \{x_i - x_j \mid i, j = 0, \dots, n, i \neq j\}$, adding a dummy variable x_0 (always equal to 0), as customary, to subsume intervals. Of course, linear templates as defined in [SSM05] are particular *P*-convex sets, for which P is given by a finite set of linear functionals.

We remark that in the case of zones, $v(x_i - x_j)$ is exactly the entry i, j of the DBM (Difference Bound Matrix) representing the corresponding zone. Also, elements of $\text{Vexp}(P \mapsto \overline{\mathbb{R}})$ corresponding naturally to *closed* DBMs, that is, canonical forms of DBMs. As is well known

[Min04], the union of two zones preserves closure whereas the intersection does not necessarily preserve closure. More generally, the set of closed elements for a Galois connection is stable under the join operation. This is reflected in our domain by (2.1) and (2.2).

3. QUADRATIC TEMPLATES

In this section, we instantiate the set P to linear and quadratic functions. This allows us to give a systematic way to derive the abstract semantics of a program. The main result is that the abstract semantics for an assignment and for a test, can be safely over-approximated by Shor’s relaxation scheme, Theorem 3.13.

Definition 3.1. We say that P is a quadratic zone iff every element template $p \in P$ can be written as:

$$x \mapsto p(x) = x^T A_p x + b_p^T x,$$

where A_p is a $d \times d$ symmetric matrix (in particular A_p can be a zero matrix), x^T denotes the transpose of a vector x , b_p is a \mathbb{R}^d vector.

Now, we suppose that P is *finite*. We denote by $\mathcal{F}(P, \mathbb{R})$ the set of functions from P to \mathbb{R} , $\mathcal{F}(P, \mathbb{R} \cup \{+\infty\})$ the set of functions from P to $\mathbb{R} \cup \{+\infty\}$ and $\mathcal{F}(P, \mathbb{R}_+)$ the set of functions from P to \mathbb{R}_+ .

Suppose now we are given a program with d variables (x_1, \dots, 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* $(x_1, \dots, x_d) = T(x_1, \dots, x_d)$, tests of the form $(x_1, \dots, x_d) \in C$, where C is some shape in $\mathcal{P}(\mathbb{R}^d)$, and while loops with similar entry tests. We do not recapitulate the standard collecting semantics that associates to this program a monotone map $F : (\mathcal{P}(\mathbb{R}^d))^n \rightarrow (\mathcal{P}(\mathbb{R}^d))^n$ whose least fixpoints $\text{lfp}(F)$ has as i th component ($i = 1, \dots, n$) the subset of \mathbb{R}^d of values that the d variables x_1, \dots, 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 $\mathcal{F}(P, \mathbb{R})^n$ to itself defined as usual as:

$$F^\sharp(v) = (F(v^*)^\dagger) \tag{3.1}$$

The notation v^* is in fact the vector of sets (v_1^*, \dots, v_n^*) and $(F(v^*)^\dagger)$ is also interpreted component-wise. The notation $\text{vexp}(v)$ will be also understood component-wise.

3.1. Shor’s semi-definite relaxation scheme. Finding the maximal value of a non-concave quadratic function under convex or non-convex quadratic constraints is known to be an *NP-Hard* problem, see [Vav90] for a discussion of complexity issues in quadratic programming. Shor’s relaxation scheme (see [TN01, Section 4.3.1] or Shor’s original article [Sho87] for details) consists of over-approximating the value of a general quadratic optimization problem by the optimal value of a semi-definite programming (SDP for short) problem, the latter being computationally more tractable.

Indeed, SDP problems can be solved in polynomial time to an arbitrary prescribed precision by the ellipsoid method [GLS88]. More precisely, let $\epsilon > 0$ be a given rational, suppose that the input data of a semi-definite program are rational and suppose that an integer N is known, such that the feasible set lies inside the ball of the radius N around

zero. Then an ϵ -optimal solution (i.e., a feasible solution the value of which is at most at a distance ϵ from the optimal value) can be found in a time that is polynomial in the number of bits of the input data and in $-\log \epsilon$. Moreover, an ϵ -solution of an SDP problem can also be found in polynomial time by interior point methods [NN94] if a strictly feasible solution is available. However, when the input is rational, no size on the bit lengths of the intermediate data is currently known, so that the term “polynomial time” for interior point methods is only understood in the model of computation over real numbers (rather than in bit model [GJ79]). The advantage of interior methods is that they are very efficient in practice. We refer the reader to [PR97] for more information.

Let $f, \{f_i\}_{i=1,\dots,m}$ be quadratic functions on \mathbb{R}^d . Let us consider the following constrained maximization problem:

$$\sup\{f(x) \mid f_i(x) \leq 0, \forall i = 1, \dots, m\} \quad (3.2)$$

In constrained optimization, it is classical to construct another constrained optimization 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 (3.2) is given by the following sup-inf (primal) value (3.3):

$$\sup_{x \in \mathbb{R}^d} \inf_{\lambda \in \mathbb{R}_+^m} f(x) - \sum_{i=1}^m \lambda_i f_i(x) . \quad (3.3)$$

A simple result of constrained optimization called weak duality theorem ensures that if we commute the inf and the sup in the formula (3.3), the result is greater than the value (3.3). The commutation of the inf and the sup gives us the so called (dual) value:

$$\inf_{\lambda \in \mathbb{R}_+^m} \sup_{x \in \mathbb{R}^d} f(x) - \sum_{i=1}^m \lambda_i f_i(x) . \quad (3.4)$$

The vectors $\lambda \in \mathbb{R}_+^m$ are called vectors of Lagrange multipliers. The function $\lambda \mapsto \sup_{x \in \mathbb{R}^d} f(x) - \sum_{i=1}^m \lambda_i f_i(x)$ is always convex and lower semi-continuous (these definitions are recalled in the appendix), so it has good properties to minimize it. If the function f is concave, 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 $i = 1, \dots, m$) holds then (3.3) and (3.4) coincide (this will be used Proposition 3.8).

Shor’s relaxation scheme consists in computing the value (3.4) by solving a semi-definite program. We introduce the matrix $M(g)$, for a quadratic function g written as $x^T A_g x + b_g^T x + c_g$ and the matrix $N(y)$ for a real y defined as:

$$M(g) = \begin{pmatrix} c_g & \frac{1}{2} b_g^T \\ \frac{1}{2} b_g & A_g \end{pmatrix}, \text{ and } N_{1,1}(y) = y, N_{i,j}(y) = 0 \text{ if } (i,j) \neq (1,1) \quad (3.5)$$

Let \preceq denote the Löwner ordering of symmetric matrices, so that $A \preceq B$ iff all eigenvalues of $B - A$ are non-negative.

When we fix $\lambda \in \mathbb{R}_+^m$, we have to maximize an unconstrained quadratic problem and the the maximum is finite iff there exists $\eta \in \mathbb{R}$ such that, for all $x \in \mathbb{R}^d$, $f(x) - \sum_{i=1}^m \lambda_i f_i(x) \leq \eta$ and since f, f_i are quadratic functions, this is equivalent to $x^T (A_f - \sum_{i=1}^m \lambda_i A_{f_i}) x + (b_f - \sum_{i=1}^m \lambda_i b_{f_i} + c_f - \sum_{i=1}^m \lambda_i c_{f_i} - \eta) \leq 0$ for all $x \in \mathbb{R}^d$ which is equivalent to the fact that the

matrix $M(f) + \eta N(-1) - \sum_{i=1}^m \lambda_i M(f_i)$ is negative semi-definite. Consequently, taking the infimum over $\lambda \in \mathbb{R}_+^m$, we recover the value (3.4).

In conclusion, Shor's relaxation scheme consists in solving the following SDP problem:

$$\text{Min}_{\substack{\lambda \in \mathbb{R}_+^m \\ \eta \in \mathbb{R}}} \eta \text{ s.t. } M(f) + \eta N(-1) - \sum_{i=1}^m \lambda_i M(f_i) \preceq 0 \quad (3.6)$$

which is equal to the value (3.4), hence an over-approximation of the optimal value of the problem (3.2). We can use a verified SDP solver as VSDP [JCK07] to solve a SDP problem.

Example 3.2. We consider the rotation of angle $\phi \in (0, \pi)$ leaving invariant the unit circle $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. We write T the linear map associated to the rotation matrix A :

$$T \begin{pmatrix} x \\ y \end{pmatrix} = A(x, y)^T = \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

where $x^2 + y^2 = 1$. To show that the proposed relaxation is accurate we next observe that it preserves the fact that the unit sphere is invariant by rotation i.e. $T(S^1) = S^1$. The inclusions $S^1 \subseteq T(S^1)$ and $T(S^1) \subseteq S^1$ can be proved by the same manner because A is an orthogonal matrix i.e. $A^T A = A A^T = Id$: $((x, y) \in S^1 \implies (x, y) \in T(S^1)) \iff (A^T(x, y) \in S^1 \text{ for } (x, y) \in S^1)$, hence, to show $S^1 \subseteq T(S^1)$ is reduced to show $T^*(S^1) \subseteq S^1$ where T^* is the linear map associated to A^T . We only prove that $T(S^1) \subseteq S^1$ and we use the Shor's relaxation scheme to prove that.

We introduce the set of quadratic functions $P = \{p_1(x, y) \mapsto x^2 + y^2, p_2(x, y) \mapsto -(x^2 + y^2)\}$ and we set $v_1(p_1) = 1$ and $v_1(p_2) = -1$. The unit sphere is the P -sub-level set of v_1 : $\{(x, y) \in \mathbb{R}^2 \mid p(x, y) \leq v_1(p), \forall p \in P\}$. To show $T(S^1) \subseteq S^1$, it suffices to show $T(v_1^*)^\dagger = v_1$. We write:

$$\begin{aligned} v_2(p_1) &:= T(v_1^*)^\dagger(p_1) = \sup\{p_1(T(x, y)) \mid p_1(x, y) \leq 1, p_2(x, y) \leq -1\} \\ v_2(p_2) &:= T(v_1^*)^\dagger(p_2) = \sup\{p_2(T(x, y)) \mid p_1(x, y) \leq 1, p_2(x, y) \leq -1\} \end{aligned}$$

For the calculus of $v_2(p_1)$, the matrices defined in 3.5 are:

$$\begin{aligned} M(p_1 \circ T) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M(p_2 \circ T) = -M(p_1 \circ T), \\ M(p_1) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad M(p_2) = -M(p_1) . \end{aligned}$$

By using the Shor's relaxation scheme, the SDP problem (3.6) gives the following equalities:

$$v_2(p_1) = \text{Min}_{\substack{\lambda(p_1) \geq 0 \\ \lambda(p_2) \geq 0 \\ \eta \in \mathbb{R}}} \eta \text{ s.t. } M(p_1 \circ T) + \eta N(-1) + \lambda(p_1)(N(1) - M(p_1)) + \lambda(p_2)(N(-1) - M(p_2)) \preceq 0$$

and

$$v_2(p_2) = \text{Min}_{\substack{\lambda(p_1) \geq 0 \\ \lambda(p_2) \geq 0 \\ \eta \in \mathbb{R}}} \eta \text{ s.t. } M(p_2 \circ T) + \eta N(-1) + \lambda(p_1)(N(1) - M(p_1)) + \lambda(p_2)(N(-1) - M(p_2)) \preceq 0$$

We can rewrite the two previous SDP problems as follows:

$$v_2(p_1) = \underset{\substack{\lambda(p_1) \geq 0 \\ \lambda(p_2) \geq 0 \\ \eta \in \mathbb{R}}}{\text{Min}} \eta \text{ s.t. } \begin{pmatrix} -\eta + \lambda(p_1) - \lambda(p_2) & 0 & 0 \\ 0 & 1 - \lambda(p_1) + \lambda(p_2) & 0 \\ 0 & 0 & 1 - \lambda(p_1) + \lambda(p_2) \end{pmatrix} \preceq 0$$

and

$$v_2(p_2) = \underset{\substack{\lambda(p_1) \geq 0 \\ \lambda(p_2) \geq 0 \\ \eta \in \mathbb{R}}}{\text{Min}} \eta \text{ s.t. } \begin{pmatrix} -\eta + \lambda(p_1) - \lambda(p_2) & 0 & 0 \\ 0 & -1 - \lambda(p_1) + \lambda(p_2) & 0 \\ 0 & 0 & -1 - \lambda(p_1) + \lambda(p_2) \end{pmatrix} \preceq 0$$

To solve these optimization problems, we could call an SDP solver, but in this case, it suffices to solve a system of inequalities: all the diagonal elements must be non-positive, for example, for the first problem, this implies that $\eta \geq 1$ and since we minimize η we get $\eta = 1$. Hence, we find $v_2(p_1) = 1$ and $v_2(p_2) = -1$ and finally we have proved $T(v_1^*)^\dagger = v_1$ and we conclude that the rotation invariance of the unit sphere $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ is preserved for the relaxation.

3.2. Abstraction of assignments and tests using Shor's relaxation.

3.2.1. *Abstraction of assignments.* We focus on assignments $(x_1, \dots, x_d) = T(x_1, \dots, x_d)$ at control point i such that $p \circ T$ is a quadratic function for every $p \in P$. Equation (3.1) translates in that case to (given that v_{i-1} defines the abstract value at control point $i-1$, i.e. immediately before the assignment):

$$(F_i^\#(v))(p) = \sup\{p \circ T(x) \mid q(x) - v_{i-1}(q) \leq 0, \forall q \in P\} . \quad (3.7)$$

We recognize the constrained optimization problem (3.2) and we use Lagrange duality as in the first step of Subsection 3.1. In our case, the Lagrange multipliers are some non-negative functions λ from P to \mathbb{R} . We thus consider the function which we will call the *relaxed* function:

$$(F_i^{\mathcal{R}}(v))(p) := \inf_{\lambda \in \mathcal{F}(P, \mathbb{R}_+)} \sup_{x \in \mathbb{R}^d} p \circ T(x) + \sum_{q \in P} \lambda(q)(v_{i-1}(q) - q(x)) . \quad (3.8)$$

To compute $F_i^{\mathcal{R}}$, we apply Shor's relaxation scheme of Subsection 3.1 and particularly the reformulation as the SDP problem (3.6), we get:

$$(F_i^{\mathcal{R}}(v))(p) = \underset{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \eta \in \mathbb{R}}}{\text{Min}} \eta \text{ s.t. } M(p \circ T) + \eta N(-1) + \sum_{q \in P} \lambda(q)(N(v_{i-1}(q)) - M(q)) \preceq 0 \quad (3.9)$$

where $M(p \circ T)$, $N(-1)$ and $M(q)$ are the matrices defined in (3.5).

We can treat the case where the map T has non-linear quadratic components. The condition $p \circ T$ is quadratic for all $p \in P$ implies, in this case, that the quadratic templates p should be linear forms which is equivalent to the fact that the matrices $M(p)$ have the following form:

$$\begin{pmatrix} 0 & \frac{1}{2}b_p^T \\ \frac{1}{2}b_p & 0 \end{pmatrix} \quad (3.10)$$

and then the matrix $\eta N(-1) + \sum_{q \in P} \lambda(q)(N(v_{i-1}(q)) - M(q))$ in Equation (3.9) has no "quadratic counterpart" (of the form of Equation (3.10), we conclude that the SDP minimization problem is feasible in this case iff $M(p \circ T)$ is negative semi-definite. Finally, the problem of Equation (3.7) is concave (since the forms $q \in P$ are linear) and consequently the Shor's relaxation scheme computes exactly the abstract semantic functional of Equation (3.7).

x	$=$	$[0, 10]$	$;$
y	$=$	1	$;$ $[1]$
xn	$=$	$-3*x*x-y*y$	$;$
yn	$=$	$-y*y+x*x$	$;$
x	$=$	xn	$;$
y	$=$	yn	$[2]$

Figure 6: A simple program written in polynomial arithmetic

Example 3.3 (Non linear assignment). Let us take a simple program written in a polynomial arithmetic (assignments now involve polynomial expressions in the variables, rather than linear ones as in the previous example). This program is described at Figure 6. We consider the set of templates $P = \{p_1, p_2\}$, with $p_1 : (x, y) \mapsto x + y$ and $p_2 : (x, y) \mapsto x - y$. We define the function T as follows:

$$(x, y) \mapsto T(x, y) = \begin{pmatrix} -3x^2 - y^2 \\ -y^2 + x^2 \end{pmatrix}$$

which is the non-linear assignment of the program described at Figure 6. By Equation (3.1), the abstract semantics are, for $w \in \mathcal{F}(P, \overline{\mathbb{R}})^2$:

$$\begin{aligned} (F_1^\sharp(w))(p) &= (11, 9) \\ (F_2^\sharp(w))(p) &= \sup_{(x,y) \in (w_1)^\star} (p \circ T)(x, y) \end{aligned}$$

About the first component of the abstract semantics, the vector $(11, 9)$ means that $(F_1^\sharp(w))(p_1) = 11$ and $(F_1^\sharp(w))(p_2) = 9$. This corresponds to the relations $x + y \leq 11$ and $x - y \leq 9$ at control point [1]. At control point [2], the relation $xn + yn = -2x^2 - 2y^2$ holds between the variables at control point [1] and [2]. In this special case, the assignments are quadratic and the templates are linear, so the evaluation of the abstract semantic functional still reduces to a (non-convex) quadratic programming problem, which, by application of Shor relaxation, leads to the following relaxed functional $(F_2^{\mathcal{R}}(w))(p_1)$ at control point 2, for an element $w \in \mathcal{F}(P, \overline{\mathbb{R}})^2$ and for the template p_1 :

$$(F_2^{\mathcal{R}}(w))(p_1) = \inf_{\substack{\lambda(q) \geq 0 \\ \forall q \in P}} \sup_{(x,y) \in \mathbb{R}^2} \sum_{q \in P} \lambda(q) w_1(q) + (x, y) \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix} (x, y)^T - \sum_{q \in P} \lambda(q) q(x, y)$$

By introducing the matrices

$$M(p_1) = \begin{pmatrix} 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0 \\ 0.5 & 0 & 0 \end{pmatrix}, \quad M(p_2) = \begin{pmatrix} 0 & 0.5 & -0.5 \\ 0.5 & 0 & 0 \\ -0.5 & 0 & 0 \end{pmatrix},$$

$$M(p_1 \circ T) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

and using Equation (3.9), we get

$$(F_2^{\mathcal{R}}(w))(p_1) = \underset{\substack{\lambda(p) \geq 0 \\ \forall p \in P \\ \eta \in \mathbb{R}}}{\text{Min}} \eta \text{ s.t. } M(p_1 \circ T) + \eta N(-1) + \sum_{q \in P} \lambda(q) (N(w_1(q)) - M(q)) \leq 0 .$$

Finally, using `Matlab`⁴, `Yalmip` [LÖ4] and `SeDuMi` [Stu99], we find $(F_2^{\mathcal{R}}(w))(p_1) = -3.2018e-09 \simeq 0$ which means, at control point [2], that $x \leq -y$ and the image of the second template by the relaxed function is $(F_2^{\mathcal{R}}(w))(p_2) = -1.0398e-09 \simeq 0$ which means, at control point [2], $x \leq y$. The invariant found $\{(x, y) \mid x \leq -y, x \leq y\}$ is an unbounded set. We can refine this set from the invariant found by interval arithmetic to get a bounded set.

3.2.2. Abstraction of simple tests. Now, we focus on a simple test and we write j the control point of the test. We assume here that a test is written as $r(x_1, \dots, x_d) \leq 0$ where r is a quadratic function. We assume that the operation for the “**then**” branch has the form $x = T_{then}(x)$ and the operation for the “**else**” branch has the form $x = T_{else}(x)$ where T_{then}, T_{else} such that $p \circ T_{then}$ and $p \circ T_{else}$ are quadratic for all $p \in P$. To enter into the “**then**” branch, the abstract values of control point $j-1$ must satisfy the test condition of the “**then**” branch, so the abstraction of a test is $F_j(X) = T_{then}(X_{j-1}) \cap \{x \in \mathbb{R}^d \mid r(x) \leq 0\}$ for the “**then**” branch. For the “**else**” branch, we have similarly $F_{j+2}(X) = T_{else}(X_{j-1}) \cap \{x \in \mathbb{R}^d \mid r(x) > 0\}$ which is equivalent to $F_{j+2}(X) = T_{else}(X_{j-1}) \cap \{x \in \mathbb{R}^d \mid -r(x) < 0\}$. However, we cannot use the Shor’s relaxation scheme with strict inequalities and so we replace the set $\{x \in \mathbb{R}^d \mid -r(x) < 0\}$ by the set $\{x \in \mathbb{R}^d \mid -r(x) \leq 0\}$ which is larger so we compute at least a safe over-approximation. When the function r is concave and the set $\{x \in \mathbb{R}^d \mid -r(x) < 0\}$ is non-empty, the closure of the former set coincides with the latter set. For the “**else**” branch, the abstraction is, finally, $F_{j+2}(X) = T_{else}(X_{j-1}) \cap \{x \in \mathbb{R}^d \mid -r(x) \leq 0\}$. As we deal with arbitrary quadratic functions r , it is sufficient to show here how to deal with the equations at control point j and we simply write T instead of T_{then} . By using Equation (3.1), we get, for $v \in \mathcal{F}(P, \overline{\mathbb{R}})^n$, and $p \in P$:

$$(F_j^{\sharp}(v))(p) = \left(T \left(v_{j-1}^* \cap \{x \in \mathbb{R}^d \mid r(x) \leq 0\} \right) \right)^{\dagger} (p)$$

then, by a simple calculus:

$$(F_j^{\sharp}(v))(p) = \sup \{ p \circ T(x) \mid q(x) \leq v_{j-1}(q) \forall q \in P, r(x) \leq 0 \}. \quad (3.11)$$

Using again the Lagrange duality, we get the relaxed problem:

$$(F_j^{\mathcal{R}}(v))(p) := \inf_{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \mu \in \mathbb{R}_+}} \sup_{x \in \mathbb{R}^d} \sum_{q \in P} \lambda(q) v_{j-1}(q) + p \circ T(x) - \sum_{q \in P} \lambda(q) q(x) - \mu r(x). \quad (3.12)$$

⁴Matlab is a registered trademark of the MathWorks, Inc.

Using the Shor's relaxation scheme described in Subsection 3.1 and in particular the SDP problem (3.6), we can rewrite $(F_j^{\mathcal{R}}(v))(p)$ as the following SDP problem:

$$\begin{array}{l} \text{Min} \\ \lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \mu \in \mathbb{R}_+ \\ \eta \in \mathbb{R} \end{array} \eta \text{ s.t. } M(p \circ T) + \eta N(-1) + \sum_{q \in P} \lambda(q) (N(v_{i-1}(q)) - M(q)) - \mu M(r) \preceq 0 \quad (3.13)$$

where $M(p \circ T)$, $N(-1)$, $M(q)$ and $M(r)$ are the matrices defined in (3.5).

```

x = [0 , 10];
y =      1;
u =      0; [ 1]
if (y*y+x*x-2<=0){
    u=x;
    x = 3-y*y;
    y = u-1; [2]
}
else {
    x=1-y*y;
    y=3-y; [ 3]
}
    
```

Figure 7: A simple program written in polynomial arithmetic

Example 3.4 (Quadratic assignment and quadratic tests). Let us take the simple program written in a polynomial arithmetic described at Figure 7. We introduce the quadratic function $r : (x, y) \mapsto y^2 + x^2 - 2$ which represents the test. We define the function T_{then} as follows:

$$(x, y) \mapsto T_{then}(x, y) = \begin{pmatrix} 3 - y^2 \\ x - 1 \end{pmatrix} .$$

We also define the function T_{else} by:

$$(x, y) \mapsto T_{else}(x, y) = \begin{pmatrix} 1 - y^2 \\ 3 - y \end{pmatrix} .$$

These two functions represent the assignments of the branches **then** and **else** respectively. Similarly to Example 3.3, we consider the domain of intervals: the set of linear templates $P = \{\underline{x}, -\underline{x}, \underline{y}, -\underline{y}\}$ where $\underline{x} : (x, y) \mapsto x$, $\underline{y} : (x, y) \mapsto y$. The abstract semantics defined by Equation (3.1) are, for $w \in \mathcal{F}(P, \overline{\mathbb{R}})^3$:

$$\begin{aligned} (F_1^\sharp(w))(p) &= \{\underline{x}(x, y) \leq 10, -\underline{x}(x, y) \leq 0, \underline{y}(x, y) \leq 1, -\underline{y}(x, y) \leq -1\}^\dagger \\ (F_2^\sharp(w))(p) &= \sup_{\substack{(x,y) \in w_1^\dagger \\ r(x,y) \leq 0}} p(T_{then}(x, y)) \\ (F_3^\sharp(w))(p) &= \sup_{\substack{(x,y) \in w_1^\dagger \\ -r(x,y) \leq 0}} p(T_{else}(x, y)) \end{aligned}$$

At the first control point, for an element $w \in \mathcal{F}(P, \overline{\mathbb{R}})^3$, the abstract semantics functional $(F_1^\sharp(w))$ takes the value 10 for the template \underline{x} , 0 for the template $-\underline{x}$, 1 for the template

\underline{y} and -1 for the template $-\underline{y}$. Again, the assignments are quadratic and the templates are linear, so the evaluation of the abstract semantic functional still reduces to a quadratic programming problem, which, by application of Shor relaxation, leads to the following relaxed functional $(F_2^{\mathcal{R}}(w))(\underline{x})$ at control point 2, for an element $w \in \mathcal{F}(P, \overline{\mathbb{R}})^3$:

$$(F_2^{\mathcal{R}}(w))(\underline{x}) = \inf_{\substack{\lambda(p) \geq 0 \\ \forall p \in P \\ \mu \in \mathbb{R}_+}} \sup_{z \in \mathbb{R}^2} \sum_{q \in P} \lambda(q) w_1(q) + z^T \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} z - \sum_{q \in P} \lambda(q) q(z) + 3 - \mu r(z)$$

By introducing the matrices

$$M(\underline{x}) = \begin{pmatrix} 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0 \\ 0.5 & 0 & 0 \end{pmatrix}, \quad M(\underline{y}) = \begin{pmatrix} 0 & 0.5 & -0.5 \\ 0.5 & 0 & 0 \\ -0.5 & 0 & 0 \end{pmatrix},$$

$$M(-\underline{x}) = -M(\underline{x}) \text{ and } M(-\underline{y}) = -M(\underline{y}),$$

$$M(r) = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M(\underline{x} \circ T_{then}) = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

and using Equation (3.9), we get

$$(F_2^{\mathcal{R}}(w))(\underline{x}) = \text{Min}_{\substack{\lambda(p) \geq 0 \\ \forall p \in P \\ \mu \in \mathbb{R}_+ \\ \eta \in \mathbb{R}}} \eta \text{ s.t. } M(\underline{x} \circ T_{then}) + \eta N(-1) - \mu M(r) + \sum_{q \in P} \lambda(q) (N(w_1(q)) - M(q)) \preceq 0$$

We find using again Yalmip, SeDuMi and Matlab, $(F_2^{\mathcal{R}}(w))(\underline{x}) = 2$. For the lower bound of the values of " $3 - y^2$ ", we find $(F_2^{\mathcal{R}}(w))(-\underline{x}) = -1$. For the variable y at control point [2], we find $(F_2^{\mathcal{R}}(w))(\underline{y}) = -3.4698e - 09 \simeq 0$ and $(F_2^{\mathcal{R}}(w))(-\underline{y}) = 1$. We remark that $(F_2^{\mathcal{R}}(w))(\underline{y}) \simeq 0$ which means that at control point [2], the values of " $x - 1$ " are less or equal to 0. Indeed, Shor's relaxation scheme detects that the test is satisfied iff $1 + x^2 - 2 \leq 0$ which is equivalent to $x^2 \leq 1$ and then the values of " $x - 1$ " are bounded by 0.

3.2.3. Properties of the relaxed semantics. We denote by \mathbb{A} the set of coordinates of the abstract semantics functional which interpret an assignment. We denote by \mathbb{I} the set of coordinates corresponding to tests (the symbol \mathbb{I} stands for "intersection"). The set of coordinates \mathbb{U} (for "union") corresponding to loops will be dealt with separately in Subsection 3.3.

Now, we are interested in the properties of the relaxed semantics which we introduced in the Subsection 3.2. First, we start by proving that the relaxed semantics is a safe over-approximation of the abstract semantics. It is deduced by the weak duality theorem: the relaxed semantics is a relaxation.

Theorem 3.5. *Let i be a coordinate in $\mathbb{A} \cup \mathbb{I}$. For all $v \in \mathcal{F}(P, \overline{\mathbb{R}})^n$,*

$$F_i^{\sharp}(v) \leq F_i^{\mathcal{R}}(v)$$

The proof is given for the convenience of the reader. We only consider the case when $i \in \mathbb{A}$ (the proof can be easily adapted to the case of tests, i.e., $i \in \mathbb{I}$).

Proof. Let $v \in \mathcal{F}(P, \overline{\mathbb{R}})^n$ and $p \in P$. If v_{i-1}^* is empty (this case includes $v_{i-1}(p) = -\infty$ for some $p \in P$), $(F_i^\sharp(v))(p) = -\infty$ for all $p \in P$ and the inequality holds. Now we suppose $v_{i-1}^* \neq \emptyset$ and we take $x \in v_{i-1}^*$. Since $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$, $\sum_{q \in P} \lambda(q)(v_{i-1}(q) - q(x)) \geq 0$ and then:

$$p \circ T(x) \leq p \circ T(x) + \sum_{q \in P} \lambda(q)(v_{i-1}(q) - q(x)) .$$

We get:

$$\sup\{p \circ T(x) \mid q(x) \leq v_{i-1}(q), \forall q \in P\} \leq \sup_{x \in \mathbb{R}^d} p \circ T(x) + \sum_{q \in P} \lambda(q)(v_{i-1}(q) - q(x)) .$$

The left-hand side does not depend on λ so we have $(F_i^\sharp(v))(p) \leq (F_i^{\mathcal{R}}(v))(p)$. \square

We observe that the calculus of the P -convex hull is a special case of assignment. Indeed, to compute a P -convex hull, is equivalent to compute the abstract effect of the assignment $x = x$. Consequently, we can apply the Shor's relaxation scheme to over-approximate the computation of the P -convex hull when the templates are quadratic.

Corollary 3.6. *Let w be in $\mathcal{F}(P, \overline{\mathbb{R}})$ and p in P we have:*

$$\begin{aligned} (\text{vex}_P(w))(p) &\leq \inf_{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \eta \in \mathbb{R}}} \eta \text{ s.t. } M(p) + \eta N(-1) + \sum_{q \in P} \lambda(q)(N(w(q)) - M(q)) \leq 0 \\ &\leq w(p) . \end{aligned}$$

Proof. The first inequality is a special case of Theorem 3.5. Let us show the second inequality. Let $w \in \mathcal{F}(P, \overline{\mathbb{R}})$ and $p \in P$. We know that the following equality holds:

$$\begin{aligned} &\inf_{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \eta \in \mathbb{R}}} \eta \text{ s.t. } M(p) + \eta N(-1) + \sum_{q \in P} \lambda(q)(N(w(q)) - M(q)) \leq 0 \\ &= \inf_{\lambda \in \mathcal{F}(P, \mathbb{R}_+)} \sup_{x \in \mathbb{R}^d} \sum_{q \in P} \lambda(q)w(q) + p(x) - \sum_{q \in P} \lambda(q)q(x) \end{aligned}$$

Let us choose $\lambda(q) = 1$ if $q = p$ and 0 otherwise. Then, $\sup_{x \in \mathbb{R}^d} \sum_{q \in P} \lambda(q)w(q) + p(x) - \sum_{q \in P} \lambda(q)q(x) = w(p)$. Since we have to take the infimum over λ so the second inequality holds. \square

The monotonicity of the relaxed semantics will be useful for the construction of Kleene iteration. Indeed, we will define in the next section a simple Kleene iteration so we show that the relaxed semantics constructed for assignments and tests define a monotone map. We adopt the convention that $\lambda(p)w(p) = 0$ if $w(p) = \infty$ and $\lambda(p) = 0$ for some $p \in P$.

Proposition 3.7. *For $i \in \mathbb{A} \cup \mathbb{I}$, the map $v \mapsto F_i^{\mathcal{R}}(v)$ is monotone on the set $\mathcal{F}(P, \overline{\mathbb{R}})^n$.*

Proof. We only give a proof for the tests so let i be in \mathbb{I} . Let v, w be in $\mathcal{F}(P, \overline{\mathbb{R}})^n$. We have for all $p \in P$, the following equality:

$$(F_i^{\mathcal{R}}(v))(p) = \inf_{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \mu \in \mathbb{R}_+}} \sum_{q \in P} \lambda(q)v_{j-1}(q) + \sup_{x \in \mathbb{R}^d} p \circ T(x) - \sum_{q \in P} \lambda(q)q(x) - \mu r(x) .$$

Since $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$, the map $v \mapsto \sum_{q \in P} \lambda(q)v_{j-1}(q)$ is monotone and since $\sup_{x \in \mathbb{R}^d} p \circ T(x) - \sum_{q \in P} \lambda(q)q(x) - \mu r(x)$ is a constant (independent of v) the function $v \mapsto F_i^{\mathcal{R}}(v)$ is an infimum of monotone maps and thus a monotone map. \square

Now we focus on a property which will be useful to construct a policy iteration for quadratic zones. We are interested in the case in which the relaxed semantics $(F_i^{\mathcal{R}}(v))(p)$ is equal to the supremum in Equation (3.8) for some λ and equal to the supremum in Equation (3.12) for some pair (λ, μ) in the case of tests. A simple condition provides the desired result: if, for all $i \in \mathbb{A} \cup \mathbb{I}$, Slater constraint qualification holds i.e. there exists $x \in \mathbb{R}^d$ such that $q(x) < v_{i-1}(q)$, $\forall q \in P$ (and for this particular x , $r(x) < 0$ holds for a test r), then there exists some λ (and a couple (λ, μ) is the case of tests) which achieves the minimum in (3.8) (the minimum in (3.12) in the case of tests). Moreover the over-approximation we make is not in general that big; in some cases, Inequality 3.5 is even an equality.

Proposition 3.8 (Selection Property). *We assume that there exist $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$ and $\mu \in \mathbb{R}_+$ such that:*

$$\sup_{x \in \mathbb{R}^d} p \circ T(x) + \sum_{q \in P} \lambda(q)(v_{i-1}(q) - q(x)) - \mu r(x)$$

is finite. If the set:

$$\{x \in \mathbb{R}^d \mid q(x) - v_{i-1}(q) < 0, \forall q \in P\} \cap \{x \in \mathbb{R}^d \mid r(x) < 0\}$$

is non-empty, then there exist $\lambda^ \in \mathcal{F}(P, \mathbb{R}_+)$ and $\mu^* \in \mathbb{R}_+$ such that:*

$$(F_i^{\mathcal{R}}(v))(p) = \sup_{x \in \mathbb{R}^d} p \circ T(x) + \sum_{q \in P} \lambda^*(q)(v_{i-1}(q) - q(x)) - \mu^* r(x)$$

Furthermore, if $p \circ T$ is a concave quadratic form and if for all $q \in P$ such that $v_{i-1}(q) < +\infty$, q is a convex quadratic form, then:

$$(F_i^{\mathcal{R}}(v))(p) = (F_i^{\sharp}(v))(p) .$$

Proof. The proof is given in the appendix. □

In the case of assignment, we can reformulate a selection property as a particular case of Proposition 3.8, since we can replace μ by 0 and remove the set $\{x \in \mathbb{R}^d \mid r(x) < 0\}$. We do not give the details for that.

Remark 3.9. We can apply Proposition 3.8 in the case of intervals, zones and linear templates: the functions $p \in P$ are all linear in these cases. When programs contain only linear expressions in assignments and tests, Proposition 3.8 implies that $F^{\sharp} = F^{\mathcal{R}}$. Unfortunately, this seems to be the only simple case in which the relaxation is exact. In other words, the linear templates of Sankaranarayanan et al. are optimal in some sense. Indeed assume there is only one quadratic template p and consider the assignment $y = T(x)$; T being affine. To evaluate the abstract semantic, we have to solve an optimisation problem of the form:

$$\begin{aligned} \text{Max} \quad & p(y) \\ \text{s.t.} \quad & y = T(x) \\ & p(x) \leq \alpha \end{aligned}$$

Due to the constraint $p(x) \leq \alpha$, the function p must be convex for the feasible set to be convex. However the same function also appears as the objective function and thus, p must be concave for the optimisation problem to be tractable by convex programming methods. This is possible only if p is affine.

The introduction of the duality provides a reformulation of Equation (3.8) and Equation (3.12): the relaxed semantics can be rewritten as the infimum of affine functions of the function v_{i-j} (when $v_{i-j}(p) \in \mathbb{R}$ for all $p \in P$). Once again, this reformulation will be useful to construct a policy iteration since it allows to solve at each step a linear program. So, let us fix $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$ and observe that the sum $\sum_{q \in P} \lambda(q)v_{i-1}(q)$ does not depend on the variable x in Equation (3.8).

Let v be in $\mathcal{F}(P, \overline{\mathbb{R}})^n$. We shall need the following notation.

- For $i \in \mathbb{A}$, we now define, for $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$, $F_i^\lambda(v)$ by:

$$(F_i^\lambda(v))(p) := \sum_{q \in P} \lambda(q)v_{i-1}(q) + V_i^\lambda(p) . \quad (3.14)$$

$$\text{where } V_i^\lambda(p) := \sup_{x \in \mathbb{R}^d} p \circ T(x) - \sum_{q \in P} \lambda(q)q(x) \quad (3.15)$$

- For $i \in \mathbb{I}$, we define, for $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$ and $\mu \in \mathbb{R}_+$, $F_i^{\lambda, \mu}(v)$ by:

$$(F_i^{\lambda, \mu}(v))(p) := \sum_{q \in P} \lambda(q)v_{i-1}(q) + V_i^{\lambda, \mu}(p) \quad (3.16)$$

$$\text{where } V_i^{\lambda, \mu}(p) := \sup_{x \in \mathbb{R}^d} p \circ T(x) - \sum_{q \in P} \lambda(q)q(x) - \mu r(x) . \quad (3.17)$$

The relaxed functional can now be readily rewritten as follows.

Lemma 3.10. *For $i \in \mathbb{A}$ and $j \in \mathbb{I}$:*

$$(F_i^{\mathcal{R}}(v))(p) = \inf_{\lambda \in \mathcal{F}(P, \mathbb{R}_+)} (F_i^\lambda(v))(p), \quad (F_j^{\mathcal{R}}(v))(p) = \inf_{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \mu \in \mathbb{R}_+}} (F_j^{\lambda, \mu}(v))(p) .$$

We remark that V_i^λ and $V_i^{\lambda, \mu}$ are the value of an unconstrained quadratic maximization problem. So, the functions V_i^λ and $V_i^{\lambda, \mu}$ can be determined algebraically. Moreover, $V_i^\lambda(p)$ and $V_i^{\lambda, \mu}(p)$ can take the value $+\infty$ if the matrices associated to the quadratic functions $x \mapsto p \circ T(x) - \sum_{q \in P} \lambda(q)q(x)$ and $x \mapsto p \circ T(x) - \sum_{q \in P} \lambda(q)q(x) - \mu r(x)$ are not negative semi-definite. Furthermore, the latter matrices depend on $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$ and on a couple $(\lambda, \mu) \in \mathcal{F}(P, \mathbb{R}_+) \times \mathbb{R}_+^d$. So, to ensure the finiteness of the value, it suffices to choose λ (or a couple (λ, μ) in the case of tests) such that the corresponding matrix is negative semi-definite. We denote by A^\bullet , the Moore-Penrose general inverse of A , which can be defined as $\lim_{\epsilon \rightarrow 0} A^T(AA^T + \epsilon Id)^{-1}$. The following proposition shows how to evaluate the functions V_i^λ and $V_i^{\lambda, \mu}$. We only consider the evaluation of $V_i^{\lambda, \mu}$ since the evaluation of the former function can be viewed as a special case of the evaluation of the latter. We recall that all the assignments T are such that $p \circ T$ is a quadratic function for all $p \in P$, and all functions r arising in tests are quadratic. Moreover, we recall that we write a quadratic function g as $x \mapsto x^T A_g x + b_g^T x + c_g$.

Proposition 3.11. *Let i be in \mathbb{I} and let an assignment T such that, for all $q \in P$, $q \circ T$ is a quadratic function. Let p be in P and let (λ, μ) be a couple in $\mathcal{F}(P, \mathbb{R}_+) \times \mathbb{R}_+$, we write:*

$$\begin{aligned} \mathcal{A}_p(\lambda, \mu) &= A_{p \circ T} - \sum_{q \in P} \lambda(q) A_q - \mu A_r \\ \mathcal{B}_p(\lambda, \mu) &= b_{p \circ T} - \sum_{q \in P} \lambda(q) b_q - \mu b_r \\ \mathcal{C}_p(\lambda, \mu) &= c_{p \circ T} - \sum_{q \in P} \lambda(q) c_q - \mu c_r \end{aligned}$$

If $(\lambda, \mu) \in \mathcal{F}(P, \mathbb{R}_+) \times \mathbb{R}_+$ satisfies $\mathcal{A}(\lambda, \mu) \preceq 0$ and $\mathcal{B}_p(\lambda, \mu) \in \text{Im}(\mathcal{A}(\lambda, \mu))$ then:

$$V_i^{\lambda, \mu}(p) = -\frac{1}{4} \mathcal{B}_p(\lambda, \mu)^T \mathcal{A}_p(\lambda, \mu) \bullet \mathcal{B}_p(\lambda, \mu) + \mathcal{C}_p(\lambda, \mu).$$

Otherwise $V_i^{\lambda, \mu}(p) = +\infty$.

The proof is classical but it is provided for the convenience of the reader.

Proof. Let $(\lambda, \mu) \in \mathcal{F}(P, \mathbb{R}_+) \times \mathbb{R}_+$ and $p \in P$. We can rewrite

$$V_i^{\lambda, \mu}(p) = \sup_{x \in \mathbb{R}^d} x^T \mathcal{A}_p(\lambda, \mu) x + \mathcal{B}_p(\lambda, \mu)^T x + \mathcal{C}_p(\lambda, \mu).$$

We assume that $\mathcal{A}(\lambda, \mu)$ is not a semi-definite matrix, there exists $y \in \mathbb{R}^d$ and $\gamma \in \mathbb{R}$, such that $\gamma^2 y^T \mathcal{A}(\lambda, \mu) y > 0$ and $\gamma \mathcal{B}_p(\lambda, \mu)^T y \geq 0$, now taking $t > 0$, we get $t\gamma^2 y^T \mathcal{A}(\lambda, \mu) y > 0$ and $t\gamma \mathcal{B}_p(\lambda, \mu)^T y \geq 0$, this leads to $V_i^{\lambda, \mu}(p) \geq ty^T \mathcal{A}_p(\lambda, \mu) y + t\gamma \mathcal{B}_p(\lambda, \mu)^T y + \mathcal{C}_p(\lambda, \mu)$ and we conclude that $V_i^{\lambda, \mu}(p) = +\infty$.

We assume that $\mathcal{A}(\lambda, \mu) \preceq 0$, the function $x \mapsto x^T \mathcal{A}_p(\lambda, \mu) x + \mathcal{B}_p(\lambda, \mu)^T x + \mathcal{C}_p(\lambda, \mu)$ is concave and differentiable then its maximum is achieved at every zero of its derivative. A maximizer \bar{x} satisfies $2\mathcal{A}_p(\lambda, \mu)\bar{x} + \mathcal{B}_p(\lambda, \mu) = 0$. If $\mathcal{B}_p(\lambda, \mu) \notin \text{Im}(\mathcal{A}(\lambda, \mu))$, the equation $2\mathcal{A}_p(\lambda, \mu)\bar{x} + \mathcal{B}_p(\lambda, \mu) = 0$ does not have a solution. Taking a non-zero vector y in the kernel of $\mathcal{A}(\lambda, \mu)$ such that $\mathcal{B}_p(\lambda, \mu)^T y > 0$, we get for all $\gamma > 0$ that $V_i^{\lambda, \mu}(p) \geq \gamma \mathcal{B}_p(\lambda, \mu)^T y + \mathcal{C}_p(\lambda, \mu)$. We conclude that $V_i^{\lambda, \mu}(p) = +\infty$. Suppose that $\mathcal{B}_p(\lambda, \mu) \in \text{Im}(\mathcal{A}(\lambda, \mu))$, then $\bar{x} = -\frac{1}{2} \mathcal{A}_p(\lambda, \mu) \bullet \mathcal{B}_p(\lambda, \mu) + z$ where z belongs to the kernel of $\mathcal{A}_p(\lambda, \mu)$. Finally, we conclude that:

$$V_i^{\lambda, \mu}(p) = -\frac{1}{4} \mathcal{B}_p(\lambda, \mu)^T \mathcal{A}_p(\lambda, \mu) \bullet \mathcal{B}_p(\lambda, \mu) + \mathcal{C}_p(\lambda, \mu)$$

since it suffices to compute $\bar{x}^T \mathcal{A}_p(\lambda, \mu) \bar{x} + \mathcal{B}_p(\lambda, \mu)^T \bar{x} + \mathcal{C}_p(\lambda, \mu)$ to find the value of $V_i^{\lambda, \mu}(p)$. \square

3.3. Abstraction of loops. The only point that we did not address yet is how to interpret the semantics equation at a control point i in which we collect the values of the variables before the entry in the body of the loop, at control point $i - 1$, with the values of the variables at the end of the body of the loop, at control point j : $F_i(X) = X_{i-1} \cup X_j$. By using Equation (3.1), for $v \in \mathcal{F}(P, \overline{\mathbb{R}})^n$, $F_i^\sharp(v) = (v_{i-1}^* \sqcup v_j^*)^\dagger$. As for zones, we notice that the union of two such P -convex functions v_{i-1} and v_j is directly given by taking their maximum on each element of the basis of quadratic functions P . Nevertheless, during the fixpoint iteration (as in Section 4) the functions v_{i-1} and v_j are not necessarily P -convex. Moreover,

if we take the abstract semantics $F_i^\sharp(v)$, we do not have an infimum of linear forms (or at least a maximum of linear forms) on the abstract values v_{i-1} and v_j , a formulation that we need. Finally, we relaxed the abstract semantics $F_i^\sharp(v)$, using Remark 2.6, by the supremum itself and $F_i^{\mathcal{R}}(v) = \sup(v_{i-1}, v_j)$. By this reduction, the map $v \mapsto F_i^{\mathcal{R}}(v)$ is monotone on $\mathcal{F}(P, \overline{\mathbb{R}})^n$. Recall that \mathbb{U} denotes the set of coordinates such that the concrete semantics is a meet operation. For $i \in \mathbb{U}$, the monotonicity of the map $v \mapsto F_i^{\mathcal{R}}(v)$ follows trivially from the previous observations. Combining this with Proposition 3.7 above, we eventually get:

Proposition 3.12. *The map $v \mapsto F^{\mathcal{R}}(v)$ is monotone on $\mathcal{F}(P, \overline{\mathbb{R}})^n$.*

To sum up, we conclude from Theorem 3.5 that we can compute over-approximations of (3.7) and (3.11) by solving a SDP problem.

Theorem 3.13. *In the case of quadratic templates, for a program with an affine arithmetics, the relaxed functional $F^{\mathcal{R}}$ can be evaluated using Shor's semi-definite relaxation and provides a sound over-approximation of the abstract functional F^\sharp .*

4. SOLVING THE SEMANTIC EQUATION

4.1. Fixpoint equations in quadratic zones. We recall that P is a finite set of quadratic templates. The map F is a monotone map which interprets a program with d variables and n labels in $(\mathcal{P}(\mathbb{R}^d))^n$. We recall that v^* denotes the vector of sets $((v_1)^*, \dots, (v_n)^*)$ and $F^\sharp(v) = (F(v^*))^\dagger$ i.e. $\forall i, F_i^\sharp(v) = (F_i(v^*))^\dagger$ 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 fixpoint equation:

$$\inf\{v \in \text{Vexp}(P \mapsto \overline{\mathbb{R}})^n \mid F^\sharp(v) \leq v\} \quad (4.1)$$

Nevertheless, the function F^\sharp is not easily computable (since the templates p are polynomials, the epigraph of F^\sharp can be checked to be a semi-algebraic set, but this of course does not lead to scalable algorithms). Hence, we solve instead the following fixpoint equation in $\mathcal{F}(P, \overline{\mathbb{R}})^n$:

$$\inf\{v \in \mathcal{F}(P, \overline{\mathbb{R}})^n \mid F^{\mathcal{R}}(v) \leq v\} \quad (4.2)$$

and sometimes, we will stop our analysis at some vectors v such that $F^{\mathcal{R}}(v) \leq v$.

We next describe and compare two ways of computing (or approximating) the smallest fixpoint of the semantic equation: Kleene iteration in Section 4.2, and policy iteration in Section 4.3.

4.2. Kleene iteration. We note by \perp the smallest element of $\text{Vexp}(P \mapsto \overline{\mathbb{R}})^n$ i.e. for all $i = 1, \dots, n$ and for all $p \in P$, $\perp_i(p) = -\infty$. The Kleene iteration sequence in $\text{Vexp}(P \mapsto \overline{\mathbb{R}})^n$ is thus as follows:

- (1) $v^0 = \perp$
- (2) for $k \geq 0$, $v^{k+1} = \text{vexp} \circ F^{\mathcal{R}}(v^k)$

Since $v \mapsto \text{vex}_P \circ F^{\mathcal{R}}$ is monotone over $\text{Vex}_P(P \mapsto \overline{\mathbb{R}})^n$, this sequence is non-decreasing, and its limit is a candidate to be the smallest fixpoint of the functional $\text{vex}_P \circ F^{\mathcal{R}}$. Unfortunately, it cannot be argued that this limit is always the smallest fixpoint without further assumptions. Indeed, $F^{\mathcal{R}}$, which is essentially defined as an infimum of affine functions, is automatically upper semi-continuous, whereas Scott continuity, i.e., lower semi-continuity in the present setting, would be required to show that the function $F^{\mathcal{R}}$ commutes with the supremum of increasing sequences. However, it can be checked that the map $\text{vex}_P \circ F^{\mathcal{R}}$ is concave (as the composition of a concave non-decreasing function, and of a concave function), and it is known that a concave function with values in $\overline{\mathbb{R}}$ is continuous on any open set on which it is finite [Roc96, Th. 10.1]. Hence, if the supremum of the sequence produced by the Kleene iteration belongs to such an open set, it is guaranteed to be the smallest fixed point. A more detailed theoretical analysis of the Kleene iteration, in the present setting of non-linear templates, appears to raise interesting technical convex analysis issues, which are beyond the scope of this paper.

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 our implementation, 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]). Note also that the P -convex hull cannot be computed exactly, so we over-approximate it using Shor relaxation. This yields an approximation of the sequence $(v^k)_{k \geq 0}$, in which the approximated vectors v^k do not belong necessarily to $\text{Vex}_P(P \mapsto \overline{\mathbb{R}})^n$ but only to $\mathcal{F}(P, \overline{\mathbb{R}})^n$.

4.3. Policy iteration algorithm.

4.3.1. *Selection property and policy iteration algorithm.* A policy iteration algorithm can be used to solve a fixpoint 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 fixpoint problems involving simpler functions.

In the present setting, we look for a representation of the relaxed function

$$F^{\mathcal{R}} = \inf_{\pi \in \Pi} F^{\pi} \tag{4.3}$$

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 $(F_i^{\mathcal{R}}(v))(p) = (F_i^{\pi}(v))(p)$. The idea of the algorithm is to start from a policy π , compute the smallest fixpoint 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 at point v .

Let us now identify the policies. Lemma 3.10 shows that for each template p , each coordinate $F_i^{\mathcal{R}}$ corresponding to an assignment $i \in \mathbb{A}$ can be written as the infimum of a family of affine functions $v \mapsto F_i^{\lambda}(v)$, the infimum being taken over the set of Lagrange

multipliers λ . The same lemma provides a representation of the same nature when the coordinate $i \in \mathbb{I}$ corresponds to a test, with now a couple of Lagrange multipliers (λ, μ) . Choosing a policy π consists in selecting, for each $i \in \mathbb{A}$ (resp. $j \in \mathbb{I}$) and $p \in P$, a Lagrange multiplier λ (resp. a pair of Lagrange multipliers λ, μ). We denote by $\pi_i(p)$ (resp. $\pi_j(p)$) the value of λ (resp. (λ, μ)) chosen by the policy π .

Then, the map F^π in (4.3) is obtained by replacing $F_i^{\mathcal{R}}$ by the affine functions appearing in Lemma 3.10, 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 Subsection 3.3).

Proposition 3.8 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 $\mathcal{F}(P, \overline{\mathbb{R}})$ 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 $i \in \mathbb{A}$ the set:

$$\{x \in \mathbb{R}^d \mid q(x) < v_{i-1}(q), \forall q \in P\}$$

and, for $i \in \mathbb{I}$ and a test r , the set:

$$\{x \in \mathbb{R}^d \mid q(x) < v_{i-1}(q), \forall q \in P\} \cap \{x \in \mathbb{R}^d \mid r(x) < 0\}$$

are non-empty.

Algorithm 1 Policy Iteration in Quadratic Templates

- 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 in Proposition 3.11 and Lemma 3.10.
 - 3 Compute the smallest fixpoint v^k in $\mathcal{F}(P, \overline{\mathbb{R}})^n$ of F^{π^k} .
 - 4 Compute $w^k = \text{vexp}(v^k)$.
 - 5 If $w^k \in \mathcal{FS}(P, \overline{\mathbb{R}})^n$ continue otherwise return w^k .
 - 6 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.
-

This leads to Algorithm 1. For the third step of Algorithm 1, since P is finite and using Lemma 3.10, F^{π^l} is monotone and affine $\mathcal{F}(P, \overline{\mathbb{R}})^n$, we compute the smallest fixpoint of F^{π^l} by solving the following linear program see [GGTZ07, Section 4]:

$$\min \sum_{i=1}^n \sum_{q \in P} v^i(q) \text{ s.t. } (F_k^{\pi^l}(v))(q) \leq v_k(q), \forall k = 1, \dots, n, \forall q \in P \quad (4.4)$$

Remark 4.1. As in the case of the earlier policy iteration algorithms in static analysis [CGG⁺05, GGTZ07], an important issue is the choice of the initial policy, which may influence the quality of the invariant which is eventually determined. In [CGG⁺05, GGTZ07], the initial policy was selected by assuming that the infimum is the expression of the functional is attained by terms corresponding to guard conditions, see specially § 4.2 in [GGTZ07]. The same principle can be used here. Another method to choose an initial policy is to run a few Kleene iterations, in combination with an acceleration technique. This leads to a postfixpoint v of $F^{\mathcal{R}}$, and we select as the initial policy any policy attaining the infimum when evaluating $F^{\mathcal{R}}(v)$ (i.e., choose for $\pi_i(p)$ or $\pi_j(p)$ any Lagrange multiplier λ or pair of Lagrange multipliers λ, μ attaining the infimum in Lemma 3.10).

Remark 4.2. To ensure the feasibility of the solution of (4.4) computed by the LP solver, we replace, when possible, the constraint set by $F^{\pi^l}(v) + \epsilon \leq v$, where ϵ is a small constant (typically of the order of several $ulp(v)$, where $ulp(v)$, which stands for “unit of least precision”, is the minimum over the coordinates i of the differences between the nearest floating points around v_i).

To obtain safe bounds even though we run our algorithm on machines which uses finite-precision arithmetic, we should use a guaranteed LP solver (e.g. LURUPA see [Kei05]) to check that the solution obtained verifies $F^{\pi^l}(v) \leq v$.

In the fourth step of Algorithm 1, the operation of closure is, in practice, the relaxation of the P -convex hull computed by a SDP solver (see Corollary 3.6). The same corollary shows that the SDP relaxation of the P -convex hull of some $w \in \mathcal{F}(P, \overline{\mathbb{R}})$, is still smaller than w and this result ensures a gain of precision.

We can only prove that policy iteration on quadratic templates converges (maybe in infinite time) towards a postfixpoint of our abstract functional and that under some technical conditions, it converges towards a fixpoint. One interest in policy iteration for static analysis is that we can always terminate the iteration after a finite time, and end up with a postfixpoint.

Theorem 4.3. *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: $F^{\mathcal{R}}(v^\infty) \leq v^\infty$.*

Proof. (1). Let $l \in \mathbb{N}$. We assume that $l > 0$ and $F^{\mathcal{R}}(v^l) \neq v^l$, there exists π^l such that, $F^{\pi^l}(v^l) = v^l$ and since $F^{\mathcal{R}} = \inf F^\pi$, we get $F^{\mathcal{R}}(v^l) \leq F^{\pi^l}(v^l) = v^l$ and from $F^{\mathcal{R}}(v^l) \neq v^l$, we conclude that $F^{\mathcal{R}}(v^l) < v^l$.

(2). We prove the second point by induction on $l \in \mathbb{N}$. We suppose that $l = 0$ if $F^{\mathcal{R}}(v^0) \neq v^0$ and that $v^0 \in \mathcal{FS}(P, \overline{\mathbb{R}})^n$ otherwise the algorithm stops. There exists π^1 such that $F^{\mathcal{R}}(v^0) = F^{\pi^1}(v^0) < v^0$ by the point 1. Moreover, v^1 is the smallest element of $\{v \in \mathcal{F}(P, \overline{\mathbb{R}})^n \mid F^{\pi^1}(v) \leq v\}$ thus $v^1 \leq v^0$ and since $F^{\pi^1}(v^0) < v^0$ we conclude that $v^1 < v^0$. The same argument holds if $v^l < v^{l-1}$ and $v^l \in \mathcal{FS}(P, \overline{\mathbb{R}})^n$.

(3). Finally, we deduce from $v^\infty \leq v^l$ that $F^{\mathcal{R}}(v^\infty) \leq F^{\mathcal{R}}(v^l) \leq v^l$. Taking the infimum over l , we get $F^{\mathcal{R}}(v^\infty) \leq v^\infty$. \square

Remark 4.4. It is desirable to choose (if possible) the initial policy π^0 so that the set:

$$\{v \in \mathcal{F}(P, \mathbb{R})^n \mid (F_i^{\pi^0}(v))(q) \leq v_i(q), \forall i = 1, \dots, n, \forall q \in P\}$$

is non-empty. Indeed, the non-emptiness of this set ensures that the coordinates of the first vector v^0 are not equal to $+\infty$ and then, by Theorem 4.3, all the terms w^k of the sequence generated by the policy iteration have coordinates which are not equal to $+\infty$. Then, the policy iteration algorithm at any step k and at any breakpoint i returns non-trivial invariants of the form $q(x) \leq \alpha$ (with $\alpha := w_i^k(q)$ finite).

Remark 4.5. The policy iteration algorithm developed in [CGG⁺05, GGTZ07] can be recovered as a special case of Algorithm 1, when applied to a domain of linear templates or to the domains of zones or intervals, for a program containing only linear expressions in assignments and tests. Indeed, the main addition in the present algorithm is the presence of the relaxation, and the latter turns out to be exact in these special cases, see Proposition 3.8.

```

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

```

$$\begin{aligned}
 F_1^\sharp(w)(p) &= \{\underline{x}(x, v) \leq 1, \underline{v}(x, v) \leq 1, \underline{L}(x, v) \leq 7\} \\
 F_2^\sharp(w)(p) &= (\sup\{w_1^*(p), w_3^*(p)\})^\dagger \\
 F_3^\sharp(w)(p) &= \sup_{(x,v) \in (w_2)^*} p(T(x, v))
 \end{aligned}$$

Figure 8: Implementation of the harmonic oscillator and its semantics in $\mathcal{F}(P, \overline{\mathbb{R}})^3$

4.4. Max strategy iteration. Gawlitza and Seidl [GS10] developed an alternative iteration to compute the least fixpoint of the relaxed semantics for the quadratic templates. The relaxed semantics which they use are constructed from the dual program of Shor’s relaxation SDP problem (3.6). Our relaxed semantics coincide with their relaxed semantics when technical conditions (which are often satisfied) hold. They obtain a map whose coordinates are the maximum of a finite number of concave functions. Their approach consists in solving the least fixpoint equation from below and they initialize their iteration by the function which is identically equal to $-\infty$. At each step of their algorithm, they select a function which achieves the maximum. Since they compute the least fixpoint from below, the least fixpoint is returned. This implies that their iteration must be run until a fixpoint is reached whereas our approach allows to stop the iteration at each step of the algorithm to provide a valid invariant. A survey [GSA⁺] recapitulates the two approaches.

4.5. A detailed calculation on the running example. Now we give details on the harmonic oscillator of Example 1. The program of this example which is given at Figure 8 implements an Euler explicit scheme with a small step $h = 0.01$, that is, which simulates the linear system $(x, v)^T = T(x, v)^T$ with

$$T = \begin{pmatrix} 1 & h \\ -h & 1 - h \end{pmatrix}$$

We want to use the information of a Lyapunov function \underline{L} of the linear system T to compute bounds on the values taken by the variables x and v of the simulation: the function $(x, v) \mapsto (x, v)L(x, v)^T$ furnishes a Lyapunov function with

$$L = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$$

We also use the quadratic functions $(x, v) \mapsto x^2$ and $(x, v) \mapsto v^2$ which corresponds to interval constraints. We introduce the set of templates $P = \{\underline{x}, \underline{v}, \underline{L}\}$ and below the program it is described the semantic equations for all the three control points. Now we are going to focus on the third coordinate of $(F^{\mathcal{R}}(v))(p)$. Let us consider, for example, $p = \underline{x}$, we get:

$$(F_3^{\mathcal{R}}(v))(x) = \inf_{\lambda \in \mathcal{F}(P, \mathbb{R}_+)} \sup_{(x,v) \in \mathbb{R}^2} \sum_{q \in P} \lambda(q) w_2(q) + (x, v) \left(\begin{pmatrix} 1 - \lambda(x) & h/2 \\ h/2 & h^2 - \lambda(v) \end{pmatrix} - \lambda(\underline{L})L \right) (x, v)^T \quad (4.5)$$

By introducing the following symmetric matrices, we can rewrite (4.5) as Equation (4.6):

$$M(\underline{x}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad M(\underline{v}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad M(\underline{x} \circ T) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & h/2 \\ 0 & h/2 & h^2 \end{pmatrix}$$

$$(F_3^{\mathcal{R}}(w))(x) = \underset{\substack{\lambda \in \mathcal{F}(P, \mathbb{R}_+) \\ \eta \in \mathbb{R}}}{\text{Min}} \eta \quad \text{s.t.} \quad M(\underline{x} \circ T) + \eta N(-1) + \sum_{q=\underline{x}, \underline{v}, \underline{L}} \lambda(q) (N(w_2(q)) - M(q)) \preceq 0 \quad (4.6)$$

To initialize Algorithm 1, we choose a policy π^0 . For the third coordinate of $F^{\mathcal{R}}$, we have to choose a policy π_3^0 such that $V_3^{\pi_3^0}(p)$ is finite for every $p = \underline{x}, \underline{v}, \underline{L}$. We can start, for example, by:

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

This consists, for $p = \underline{x}$, in taking $\lambda(\underline{x}) = \lambda(\underline{v}) = 0$ and $\lambda(\underline{L}) = 1$ in (4.5). By Proposition 3.11 we find:

$$V_3^{\pi_3^0}(\underline{x}) = \sup_{(x,v) \in \mathbb{R}^2} (x, v) \begin{pmatrix} -1 & h/2 - 1 \\ h/2 - 1 & h^2 - 3 \end{pmatrix} (x, v)^T = 0$$

$$V_3^{\pi_3^0}(\underline{v}) = \sup_{(x,v) \in \mathbb{R}^2} (x, v) \begin{pmatrix} h^2 - 2 & h(1-h) - 1 \\ h(1-h) - 1 & (1-h)^2 - 3 \end{pmatrix} (x, v)^T = 0$$

$$V_3^{\pi_3^0}(\underline{L}) = \sup_{(x,v) \in \mathbb{R}^2} (x, v) (T^T L T - L) (x, v)^T = 0$$

The solution of the maximization problems are zero since all the three matrices are negative definite (i.e. a matrix B is negative definite iff $x^t A x < 0$ for all $x \neq 0$). The third matrix $T^T L T - L$ is negative definite since L satisfy the Lyapunov condition for the discrete linear system $(x, v) = T(x, v)$. To compute the least fixpoint of F^{π^0} , we solve the following linear program (see (4.4)):

$$\min \sum_{i=1}^3 \sum_{p \in P} \beta_i(p)$$

$$\beta_2(\underline{L}) \leq \beta_3(\underline{x}), \quad \beta_2(\underline{L}) \leq \beta_3(\underline{v}), \quad \beta_2(\underline{L}) \leq \beta_3(\underline{L})$$

$$\beta_3(\underline{x}) \leq \beta_2(\underline{x}), \quad \beta_3(\underline{v}) \leq \beta_2(\underline{v}), \quad \beta_3(\underline{L}) \leq \beta_2(\underline{L})$$

$$1 \leq \beta_2(\underline{x}), \quad 1 \leq \beta_2(\underline{v}), \quad 7 \leq \beta_2(\underline{L})$$

$$1 \leq \beta_1(\underline{x}), \quad 1 \leq \beta_1(\underline{v}), \quad 7 \leq \beta_1(\underline{L})$$

Using solver `Linprog`, we find:

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

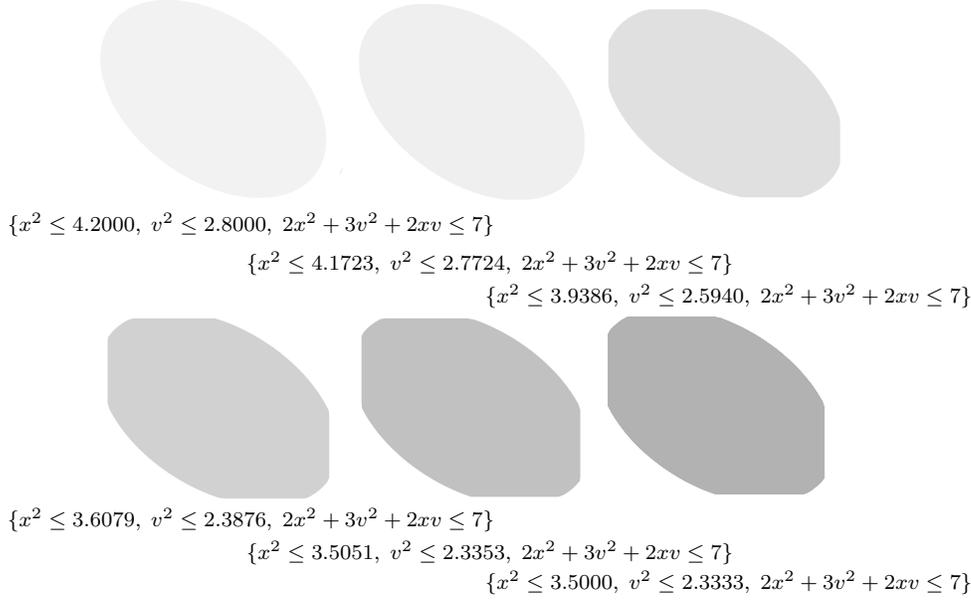


Figure 9: Successive templates along policy iteration, at control point 2, for the harmonic oscillator.

The approximation of the closure of u^0 , $\text{vexp}(u^0)$ is given by a `Matlab` implementation, using `Yalmip` and `SeDuMi` returns the vector w_1^0 :

$$\begin{array}{lll}
 w_1^0(\underline{x}) = 1.0000 & w_2^0(\underline{x}) = 4.2000 & w_3^0(\underline{x}) = 4.2000 \\
 w_1^0(\underline{v}) = 1.0000 & w_2^0(\underline{v}) = 2.8000 & w_3^0(\underline{v}) = 2.8000 \\
 w_1^0(\underline{L}) = 7.0000 & w_2^0(\underline{L}) = 7.0000 & w_3^0(\underline{L}) = 7.0000
 \end{array}$$

Using again `Yalmip` with the solver `SeDuMi`, the vector w is not a fixpoint of $F^{\mathcal{R}}$, so we get the new following policy:

$$\pi_3^1(\underline{x}) = (0, 0, 0.596), \quad \pi_3^1(\underline{v}) = (0, 0, 0.3961), \quad \pi_3^1(\underline{L}) = (0, 0, 0.9946) .$$

Finally, after 5 iterations we find that the invariant of the loop i.e. w_2^* at control point 2 is the set:

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

We draw w_2^* at each iteration of Algorithm 1 in Figure 9.

This method is to be compared with the classical Kleene iteration with widening. On this example, we find without widening $x^2 \leq 3.5000, v^2 \leq 2.3333$ and $2x^2 + 3v^2 + 2xv \leq 7$ in 1188 iterations whereas with the acceleration technique described Subsection 4.2 we find $x^2 \leq 6.0000, v^2 \leq 4.0000$ and $2x^2 + 3v^2 + 2xv \leq 10$ in 15 iterations.

5. BENCHMARKS

We implemented an analyzer for the quadratic template domain we presented, written in `Matlab` version 7.8(R2009a). This analyzer takes a text file in argument. This text file corresponds to the abstract equation $v = F^\sharp(v)$ where F^\sharp is defined by Equation (2.4). The

Programs	Method	#P	#lines	#var	#loops	#Iter.	Inv. quality	Time (s)
Rotation2	Policy	2	2	2	0	0	Fixpoint	2.85
Rotation2	Kleene	2	2	2	0	2	Fixpoint	2.87
Rotation10	Policy	2	2	10	0	0	Fixpoint	2.85
Rotation10	Kleene	2	2	10	0	2	Fixpoint	3.04
Filter	Policy	5	3	2	1	3	Fixpoint	9.93
Filter	Kleene	5	3	2	1	15	Postfixpoint	64.03
Oscillator	Policy	3	3	2	1	5	Fixpoint	9.92
Oscillator	Kleene	3	3	2	1	15	Fixpoint	38.91
Oscillatorc2	Policy	3	3	4	1	5	Fixpoint	10.09
Oscillatorc2	Kleene	3	3	4	1	15	Postfixpoint	40.54
Oscillatorc5	Policy	3	3	10	1	5	Fixpoint	11.43
Oscillatorc5	Kleene	3	3	10	1	16	Fixpoint	57.33
Oscillatorc10	Policy	3	3	20	1	6	Fixpoint	22.03
Oscillatorc10	Kleene	3	3	20	1	20	Postfixpoint	161.43
Oscillatorc20	Policy	3	3	40	1	6	Fixpoint	236.40
Oscillatorc20	Kleene	3	3	40	1	20	Fixpoint	1556.90
Symplectic	Policy	5	3	2	1	0	Fixpoint	4.22
Symplectic	Kleene	5	3	2	1	15	Fixpoint	66.14
SymplecticSeu	Policy	5	3	2	1	5	Postfixpoint	12.79
SymplecticSeu	Kleene	5	3	2	1	15	Postfixpoint	66.02

Figure 10: Benchmarks

quadratic template can be loaded from a `dat` file by the analyzer. The affine maps are treated in the same manner.

In this analyzer, we can choose to use the Kleene iteration method or policy iteration. For the Kleene iteration method, the user gives as an argument a maximal number of iteration and if the acceleration method has to be applied. The acceleration method start from the iteration $n+1$ (n denotes the number of lines of the code) and ends eleven iteration after. For the policy iteration method, the user gives the `dat` file defining the initial policy or chooses to make Kleene iterations before determining the initial policy.

For the policy iteration, the user gives also as argument a maximal number of iteration and the policy iteration runs until a fixpoint is reached or Slater constraint qualification is no longer satisfied or if the maximal number of iteration is achieved and so a postfixpoint can be returned by the policy iteration algorithm. Similarly, the Kleene iteration with acceleration provides a postfixpoint after acceleration and widening to top, if the iteration does not converge after a given number of iterations. The analyzer writes, in a text file, information about time, quality of the invariants found and number of iterations.

For the benchmarks, we used a single core of a laptop PC Intel(R) Duo CPU P8600 at 2.4 Ghz with a main memory of 4Gb. We indicate in Table 10, the name of the program analyzed, the method used (policy iteration or Kleene iteration) for solving the fixpoint equation, the cardinality of the basis of quadratic templates used, the number of lines of C code the program has, the number of variables it manipulates, the number of loops. Then we indicate the number of iterations made, whether it reaches a fixpoint or (strictly) a postfixpoint. Finally, the last column concerns the time in seconds to compute the invariant.

```

x = [0 , 1];
y = [0 , 1]; [1]
while [2] (true) {
  x = (3/4)*x - (1/8)*y;
  y = x; [3]
}

```

Figure 11: The program Filter

The file Rotation10 is the problem of Example 3.2 in dimension 10. By the fixpoint computation, we prove automatically that the unit sphere in dimension 10 is invariant by rotation. Both Kleene iteration and policy iteration find the unit sphere as invariant.

The program Filter is an implementation of recursive linear filter of second order. The program is described Figure 11. By policy iteration, we find the following set as loop invariant (at control point 2):

$$\{-0.5 \leq x \leq 1, -0.5 \leq v \leq 1, 3x^2 + v^2 \leq 4\} .$$

Although, the Kleene iteration with acceleration finds the following set:

$$\{-1.8257 \leq x \leq 1.8257, -3.1623 \leq v \leq 3.1623, 3x^2 + v^2 \leq 10\} .$$

The program Oscillator is the problem 1. The invariant depicted Figure 1 in Section 1 is found by policy iteration whereas Kleene iteration after applying acceleration techniques from the iteration 4 to iteration 15 finds the less precise invariant $\{x^2 \leq 6.0000, v^2 \leq 4, 2x^2 + 3v^2 + 2xv \leq 10\}$, in more time.

In order to illustrate the scalability of the method, we considered a higher dimensional analogue of the example of Figure 1, modelling N coupled harmonic oscillators, $\ddot{x}_i + \dot{x}_i + x_i + \epsilon \sum_{1 \leq j \leq N} x_j = 0$, for $1 \leq i \leq N$. Hence, N variables x_i , v_i , and w_i now appear in the discretised scheme instead of x, v, w . We computed automatically a Lyapunov function in **Matlab**. We used as templates the one arising from the latter Lyapunov function, together with $\sum_{i=1}^N x_i^2$ and $\sum_{i=1}^N v_i^2$. We took $\epsilon = 0.5$. We made tests successively for $N = 2, 5, 10, 20$ (Oscillatorc2, Oscillatorc5, Oscillatorc10 and Oscillatorc20). As in the program Oscillator, we were interested in the loop invariant. For example, for $N = 20$, we found with policy iteration algorithm the following set:

$$\{(x, v) \in \mathbb{R}^{20} \times \mathbb{R}^{20} \mid \sum_{i=1}^{20} x_i^2 \leq 115.7169, \sum_{i=1}^{20} v_i^2 \leq 266.3048, (x, v)L(x, v)^T \leq 350.0690\}$$

where L denotes positive semi-definite matrix associated to the Lyapunov function found automatically by **Matlab**.

The Symplectic example implements a discretisation of $\ddot{x} + c\dot{x} + x = 0$ with $c = 0$ by a symplectic method, considering specially the case in which $c = 0$ (there is no damping). Then, the dynamical system has imaginary eigenvalues (its orbits are circles), reflecting the fact that energy is constant. However, the Euler scheme, which does not preserve this conservation law, diverges, so we use a symplectic discretisation scheme (preserving the symplectic form, see [HLW03]). This is an interesting, highly degenerate, numerical example from the point of view of static analysis, because there is no “stability margin”, hence, methods not exploiting the Lyapunov function are likely to produce trivial invariants when $c = 0$. As in Oscillator, we start from a position $x \in [0, 1]$ and a speed $v \in [0, 1]$.

```

tau = 0.1;
x = [0 , 1];
v = [0 , 1]; [1]
while [2] (true) {
  x = (1-(tau/2))*x+(tau-((tau^3)/4))*v;
  v = -tau*x+(1-(tau/2))*v; [3]
}

```

Figure 12: An implementation of the symplectic method

The discretisation of $\ddot{x} + x = 0$ with the symplectic method and a step $\tau = 0.1$ gives us the matrix T such that $T_{1,1} = 1 - \frac{\tau}{2}$, $T_{1,2} = \tau - \frac{\tau^3}{4}$, $T_{2,1} = -\tau$ and $T_{2,2} = 1 - \frac{\tau}{2}$. We use the Lyapunov function L such that $L(x, v) = (x, v)Q(x, v)^T$ with

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 - \frac{\tau^2}{4} \end{pmatrix} .$$

The symplectic method ensures that $L(T(x, v)) = L(x, v)$. Our method takes advantage of this conservation law, since L is embedded as a template. The policy iteration returns the following as invariant set at the control point 2:

$$\{-1.41333 \leq x \leq 1.41333, -1.4151 \leq v \leq 1.4151, x^2 + 0.9975v^2 \leq 1.9975\} .$$

Whereas the Kleene iteration returns:

$$\{-3.16624 \leq x \leq 3.16624, -3.16628 \leq v \leq 3.16628, x^2 + 0.9975v^2 \leq 10\} .$$

which is less precise. In particular, the Kleene algorithm misses the invariance of the Lyapunov function.

SymplecticSeu is a symplectic method with a threshold on $v = \dot{x}$. We iterate the Symplectic method while $v \geq \frac{1}{2}$, which gives the following code:

```

x = [0 , 1];
v = [0 , 1];
tau = 0.1 [1]
while [2] ((v >= 1/2)) {
  x = (1-tau/2)*x+(tau-(tau^3)/4)*v;
  v = -tau*x+(1-tau/2)*v; [3]
};

```

The policy iteration returns the following set which the invariant found at control point 2:

$$\{0 \leq x \leq 1.3654, 0 \leq v \leq 1, x^2 + 0.9975v^2 \leq 1.9975\} .$$

and the policy iteration returns the following set at control point 3:

$$\{0.0499 \leq x \leq 1.3222, 0.5 \leq v \leq 0.9950, x^2 + 0.9975v^2 \leq 1.9975\} .$$

Although, the Kleene iteration with acceleration provides the following set which the invariant found at control point 2:

$$\{0 \leq x \leq 3.1623, 0 \leq v \leq 3.1662, x^2 + 0.9975v^2 \leq 10\} .$$

and the same set at the control point 3.

Remark 5.1. In the present benchmarks, the execution time of a single policy iteration step and of a single Kleene iteration step are comparable (the acceleration provided by policy iteration comes from the smaller number of iterations). Indeed, at each Kleene or Policy iteration, the bottleneck appears to be the evaluation of the relaxed functional $F^{\mathcal{R}}$, which requires to solve a family a Shor SDP relaxations. Policy iteration requires in addition to solve a family of linear programs (to compute the smallest fixpoint of the current policy). This is technically easier than solving the SDPs, and generally faster. However, each SDPs is typically local (involving a small number of variables), whereas the linear programs, which couple all the breakpoints and all the templates functions, may be of large size. Hence, one may construct (very large) instances in which solving the linear programs would become the bottleneck.

6. CONCLUSION AND FUTURE WORK

We have presented in this paper a generalization of the linear templates of Sankaranarayanan et al. [SSM05, SCSM06] allowing one to deal with non-linear templates. We showed that in the case of quadratic templates, we can efficiently abstract the semantic functionals using Shor’s relaxation, and compute the resulting fixpoint using policy iteration. Future work include the use of tighter relaxations for quadratic problems. In particular, sum of squares (SOS) relaxations (see for instance [Las07] and [Par03]) would allow us to obtain more accurate safe over-approximation of the abstract semantic functional for arbitrary polynomial templates and for a general program arithmetics. Kleene iteration could be easily implemented in that way. However, the issue of coupling SOS relaxations with policy iteration appears to be more difficult. Note also that unlike Shor relaxation, SOS relaxations are subject to a “curse of dimensionality”. These issues will be examined further elsewhere. Another problem is to extend the minimality result of [AGG08] which is currently only available for the interval domain, to our template domain. We intend to study more in-depth the complexity issues raised by our general policy iteration algorithm. Finally, we note that a more detailed account of the present work has appeared in the Phd thesis of the first author [Adj11].

ACKNOWLEDGEMENT.

We thank Thomas Gawlitza and David Monniaux for their remarks on an earlier version of this paper. We also thank the three referees for their careful reading and comments.

REFERENCES

- [Adj11] A. Adjé. *Optimisation et jeux appliqués à l’analyse statique de programme par interprétation abstraite*. Phd thesis, École Polytechnique, April 2011.
- [AGG08] A. Adje, S. Gaubert, and E. Goubault. Computing the smallest fixed point of nonexpansive mappings arising in game theory and static analysis of programs. Technical report, arXiv:0806.1160, Proceedings of MTNS’08, Blacksburg, Virginia, July 2008.
- [AGG10] 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.

- [AT03] A. Auslender and M. Teboulle. *Asymptotic Cones and Functions in Optimization and Variational Inequalities*. Springer, 2003.
- [BRCZ05] R. Bagnara, E. Rodríguez-Carbonell, and E. Zaffanella. Generation of basic semi-algebraic invariants using convex polyhedra. In C. Hankin, editor, *Static Analysis: Proceedings of the 12th International Symposium*, volume 3672 of *LNCS*, pages 19–34. Springer, 2005.
- [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.
- [Cou05] P. Cousot. Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming. In *Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05)*, volume 3385 of *LNCS*, pages 1–24. Springer, 2005.
- [DP02] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, New York, second edition, 2002.
- [FA08] E. Feron and F. Alegre. Control software analysis, part II: Closed-loop analysis. Technical report, arXiv:0812.1986, 2008.
- [Fer05] J. Feret. Numerical abstract domains for digital filters. In *International workshop on Numerical and Symbolic Abstract Domains (NSAD 2005)*, 2005.
- [FF08] E Feron and Alegre F. Control software analysis, part I: Open-loop properties. Technical report, arXiv:0809.4812, 2008.
- [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.
- [GJ79] M. R. Garey and D. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H.Freeman & Co Ltd, 1979.
- [GLS88] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer, 1988.
- [GPBG08] E. Goubault, S. Putot, P. Baufreton, and J. Gassino. Static analysis of the accuracy in control systems: Principles and experiments. In *Formal Methods for Industrial Critical System (FMICS 2007)*, volume 4916 of *LNCS*, pages 3–20, 2008.
- [GS07a] T. Gawlitza and H. Seidl. Precise fixpoint computation through strategy iteration. In R. De Nicola, editor, *Programming Languages and Systems, 16th European Symposium on Programming, ESOP 2007*, volume 4421 of *LNCS*, pages 300–315. Springer, 2007.
- [GS07b] T. Gawlitza and H. Seidl. Precise relational invariants through strategy iteration. In Jacques Duparc and Thomas A. Henzinger, editors, *Computer Science Logic, 21st International Workshop, CSL 2007, 16th Annual Conference of the EACSL, Lausanne, Switzerland, September 11-15, 2007, Proceedings*, volume 4646 of *LNCS*, pages 23–40. Springer, 2007.
- [GS10] T. M. Gawlitza and H. Seidl. Computing relaxed abstract semantics w.r.t. quadratic zones precisely. In Radhia Cousot and Matthieu Martel, editors, *SAS*, volume 6337 of *Lecture Notes in Computer Science*, pages 271–286. Springer, 2010.
- [GSA⁺] T. Gawlitza, H. Seidl, A. Adjé, S. Gaubert, and E. Goubault. Abstract interpretation meets convex optimization. To appear in *Journal of symbolic computation*, Special issue on invariant generation and advanced techniques for reasoning about loops.
- [HLW03] E. Hairer, C. Lubich, and G. Wanner. Geometric numerical integration illustrated by the Störmer/Verlet method. *Acta Numerica*, 12:399–450, 2003.
- [JCK07] C. Jansson, D. Chaykin, and C. Keil. Rigorous error bounds for the optimal value in semidefinite programming. *SIAM J. Numer. Anal.*, 46(1):180–200, 2007.
- [Kei05] C. Keil. Lurupa - rigorous error bounds in linear programming. In *Algebraic and Numerical Algorithms and Computer-assisted Proofs*, 2005. <http://drops.dagstuhl.de/opus/volltexte/2006/445>.

- [LÖ4] J. Löfberg. Yalmip : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004. <http://control.ee.ethz.ch/~joloef/yalmip.php>.
- [Las07] J.-B. Lasserre. A sum of squares approximations of nonnegative polynomials. *SIAM Review*, 49(4):651–669, 2007.
- [LGG09] C. Le Guernic and A. Girard. Reachability analysis of hybrid systems using support functions. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification*, volume 5643 of *Lecture Notes in Computer Science*, pages 540–554. Springer Berlin / Heidelberg, 2009.
- [Min04] A. Miné. *Weakly Relational Numerical Abstract Domains*. PhD thesis, École Polytechnique, Palaiseau, France, December 2004. <http://www.di.ens.fr/~mine/these/these-color.pdf>.
- [Mor70] J. J. Moreau. Inf-convolution, sous-additivé, convexité des fonctions numériques. *Journal Mathématiques de Pures et Appliquées*, 49:109–154, 1970.
- [MOS04] M. Müller-Olm and H. Seidl. Computing polynomial program invariants. *Inf. Process. Lett.*, 91(5):233–244, 2004.
- [NN94] Y. Nesterov and A. Nemirovski. *Interior point polynomial algorithms in convex programming*. Society for Industrial and Applied Mathematics, 1994.
- [Par03] P. Parillo. Semidefinite programming relaxations for semialgebraic problems. *Math. Prog.*, 96(2, series B):293–320, 2003.
- [PR97] P.M. Pardalos and M.V. Ramana. Semidefinite programming. In *Interior Point Methods of Mathematical Programming*, pages 369–398. Kluwer Academic Publishers, 1997.
- [RCK07] E. Rodríguez-Carbonell and D. Kapur. Automatic generation of polynomial invariants of bounded degree using abstract interpretation. *Sci. Comput. Program.*, 64(1):54–75, 2007.
- [Roc96] R.T. Rockafellar. *Convex Analysis*. Princeton University Press, 1996.
- [Rub00] A. M. Rubinov. *Abstract Convexity and Global optimization*. Kluwer Academic Publishers, 2000.
- [SCSM06] S. Sankaranarayanan, M. Colon, H. Sipma, and Z. Manna. Efficient strongly relational polyhedral analysis. In E. Allen Emerson and Kedar S. Namjoshi, editors, *Verification, Model Checking, and Abstract Interpretation: 7th International Conference, (VMCAI)*, volume 3855 of *LNCS*, pages 111–125, Charleston, SC, January 2006. Springer.
- [Sho87] N. Shor. Quadratic optimization problems. *Soviet J. of Computer and Systems Science*, 25(6):1–11, 1987.
- [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 *Sixth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05)*, volume 3385 of *LNCS*, pages 25–41, January 2005.
- [Stu99] J. F. Sturm. Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11-12:625–653, 1999.
- [TN01] A. Ben Tal and A. Nemirovski. *Lecture on Modern Convex Optimization: Analysis, Algorithm and Engineering Applications*. SIAM, 2001.
- [Vav90] Stephen A. Vavasis. Quadratic programming is in NP. *Information Processing Letters*, 36(2):73–77, 1990.

APPENDIX

Let f be a function from \mathbb{R}^d to $\mathbb{R} \cup \{+\infty\}$. We say that the function f is proper iff there exists $x \in \mathbb{R}^d$ such that $f(x) \in \mathbb{R}$.

We recall that f is convex iff the set $\text{epi}(f) := \{(x, \alpha) \in \mathbb{R}^d \times \mathbb{R} \mid f(x) \leq \alpha\}$ is a convex set (i.e. for all $t \in [0, 1]$, for all $x, y \in \text{epi}(f)$, $tx + (1-t)y \in \text{epi}(f)$). Since the intersection of a family of convex sets is a convex set then the pointwise supremum of a family of convex functions is also a convex function.

The function f is said to be lower semi-continuous iff the sets $\{x \in \mathbb{R}^d \mid f(x) \leq \alpha\}$ are (topologically) closed for all $\alpha \in \mathbb{R}$. Since the intersection of a family of closed sets is closed set then the pointwise supremum of a family of lower semi-continuous functions is also a lower semi-continuous function.

The function f is level-bounded iff $\{x \in \mathbb{R}^d \mid f(x) \leq \alpha\}$ are bounded set for all $\alpha \in \mathbb{R}$. If $\lim_{\|x\| \rightarrow +\infty} f(x) = +\infty$ then f is level-bounded.

Proposition 3.8 is deduced from a well-known result of convex optimization:

Proposition 6.1. *Let $f : \mathbb{R}^d \mapsto \mathbb{R} \cup \{+\infty\}$ be a convex, proper, lower semi-continuous and level bounded function. Then $\inf_{x \in \mathbb{R}^d} f(x)$ is finite and there exists \bar{x} such that:*

$$f(\bar{x}) = \inf_{x \in \mathbb{R}^d} f(x) .$$

A proof of Proposition 6.1 can be found in [AT03, Proposition 3.1.3].

Proof of Proposition 3.8. We begin the proof by writing:

$$g(\lambda, \mu) = \begin{cases} \sup_{x \in \mathbb{R}^d} p \circ T(x) + \sum_{q \in P} \lambda(q)(v_{i-1}(q) - q(x)) - \mu r(x) & \text{if } \lambda \in \mathcal{F}(P, \mathbb{R}_+), \mu \in \mathbb{R}_+ \\ +\infty & \text{otherwise} \end{cases}$$

To show Proposition 3.8, it suffices to show that the hypothesis of Proposition 6.1 are verified: the function g is convex, lower semi-continuous, proper and level-bounded.

The set P is finite so $\mathcal{F}(P, \mathbb{R})$ is the finite dimensional vector space $\mathbb{R}^{|P|}$ where $|P|$ is the cardinality of P . First, the function g is convex and lower-continuous as the pointwise supremum of convex continuous functions.

The function g is also proper since $g(\lambda, \mu) > -\infty$, for all $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$, for all $\mu \in \mathbb{R}_+$ and there exist $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$ and $\mu \in \mathbb{R}_+$ such that $g(\lambda, \mu) < +\infty$.

The function g is level-bounded since $\lambda \in \mathcal{F}(P, \mathbb{R}_+)$, $\mu \in \mathbb{R}_+$ and there exists some $\bar{x} \in \mathbb{R}^d$ such that, for all $q \in P$, $v_{i-1}(q) - q(\bar{x}) > 0$ and $r(\bar{x}) < 0$, we conclude that $g(\lambda, \mu) \geq p \circ T(\bar{x}) + \min_{q \in P} (v_{i-1}(q) - q(\bar{x})) \sum_{q \in P} \lambda(q) - r(\bar{x})\mu$ then $g(\lambda, \mu)$ tends to $+\infty$ as $\max(\|\lambda\|_1, |\mu|)$ tends to ∞ .

The second part of Proposition 3.8 follows from the strong duality theorem for convex optimization problems, see e.g. [AT03, Proposition 5.3.2]. \square