Department of Mathematics, University of Parma, Italy
Quaderno 458

Applications of Polyhedral Computations to the Analysis and Verification of Hardware and Software Systems

Roberto Bagnara, Patricia M. Hill, and Enea Zaffanella

ABSTRACT. Convex polyhedra are the basis for several abstractions used in static analysis and computer-aided verification of complex and sometimes mission critical systems. For such applications, the identification of an appropriate complexity-precision trade-off is a particularly acute problem, so that the availability of a wide spectrum of alternative solutions is mandatory. We survey the range of applications of polyhedral computations in this area; give an overview of the different classes of polyhedra that may be adopted; outline the main polyhedral operations required by automatic analyzers and verifiers; and look at some possible combinations of polyhedra with other numerical abstractions that have the potential to improve the precision of the analysis. Areas where further theoretical investigations can result in important contributions are highlighted.

1. Introduction

The application of polyhedral computations to the analysis and verification of computer programs has its origin in a groundbreaking paper by Cousot and Halbwachs [CH78]. There, the authors applied the theory of abstract interpretation [CC77] to the static determination of linear equality and inequality relations among program variables. Essentially, the idea consists in interpreting the program (as will be explained in more detail in Sections 2.1 and 3) on a domain of convex polyhedra instead of the concrete domain of (sets of vectors of) machine numbers. Each program operation is correctly approximated by a corresponding operation on polyhedra and measures are taken to ensure that the approximate computation always terminates. At the end of this process, the obtained polyhedra encode provably correct *linear invariants* of the analyzed program (i.e., linear equalities and inequalities that are guaranteed to hold for each program execution and for each program input).

As we show in this paper, relational information concerning the data objects manipulated by programs or other devices is crucial for a broad range of applications in the field of automatic or semi-automatic program manipulation: it can

---

2000 *Mathematics Subject Classification.* Primary 68Q60, 52B99; Secondary 68N30, 68Q55.
Key words and phrases. Static analysis, computer-aided verification, abstract interpretation.
This work has been partly supported by PRIN project "AIDA: Abstract Interpretation Design and Applications."

be used to prove the absence of certain kinds of errors; it can verify that certain processes always terminate or stabilize, it can pinpoint the position of errors in the system, and it can enable the application of optimizations. Despite this, due to the lack of efficient, robust and publicly available implementations of convex polyhedra and of the required operations, the line of work begun by Cousot and Halbwachs did not see much development until the beginning of the 1990s. Since then, this approach has been increasingly adopted and today convex polyhedra are the basis for several abstractions used in static analysis and computer-aided verification of complex and sometimes mission critical systems. For such applications, the identification of an appropriate complexity-precision trade-off is a particularly acute problem: on the one hand, relational information provided by general polyhedra is extremely valuable; on the other hand, its high computational cost makes it a fairly scarce resource that must be managed with care. This implies, among other things, that general polyhedra must be combined with simpler polyhedra in order to achieve scalability. As the complexity-precision trade-off varies considerably between different applications, the availability of a wide spectrum of alternative solutions is mandatory.

In this paper, we survey the range of applications of polyhedral computations in the area of the analysis and verification of hardware and software systems: we describe in detail one important —and historically, first— application of polyhedral computation in the field of formal methods, the linear invariant analysis for imperative programs; we provide an account of linear hybrid systems that is based directly on polyhedra; and we show how polyhedral approximations can be applied to analog systems. The paper also provides an overview of the main polyhedral operations required by these applications, brief descriptions of some of the different classes of polyhedra that may be adopted, depending on the particular context, and a look at some possible combinations of polyhedra with other numerical abstractions that have the potential to improve the precision of the analysis. Areas where further theoretical investigations can result in important contributions are highlighted.

The plan of the paper is as follows. Section 2 introduces the required notions and notations, including a minimal exposition of the main concepts of abstract interpretation theory. Section 3 demonstrates the use of polyhedral computations in the specification of a linear invariant analysis for a simple imperative language; a few of the many applications for the analysis of computer programs are briefly recalled. Section 4 is devoted to polyhedral approximation techniques for hybrid systems, which, as shown in Section 5 can also be applied to purely analog systems. Section 6 presents several families of polyhedral approximations that provide a range of different solutions to the complexity/precision trade-off. The most important operations that such approximations must provide in order to support analysis and verification methods are illustrated in Section 7. Section 8 concludes.

2. Preliminaries

We assume some basic knowledge about lattice theory [Bir67]. Let $(S, \sqsubseteq)$ and $(T, \preceq)$ be two partially ordered sets; the function $f \colon S \to T$ is *monotonic* if, for all $x_0, x_1 \in S$, $x_0 \sqsubseteq x_1$ implies $f(x_0) \preceq f(x_1)$. If $(S, \sqsubseteq) \equiv (T, \preceq)$, so that $f \colon S \to S$, an element $x \in S$ such that $x = f(x)$ is a *fixpoint* of f. If $(S, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$ is a complete lattice, then f is *continuous* if it preserves the least upper bound of all increasing chains, i.e., for all $x_0 \sqsubseteq x_1 \sqsubseteq \cdots$ in S, it satisfies $f\bigl(\bigsqcup x_i\bigr) = \bigsqcup f(x_i)$; in such a case, the least fixpoint of f with respect to the partial order '$\sqsubseteq$', denoted $\operatorname{lfp} f$, can be obtained by iterating the application of f starting from the bottom element $\bot$, thereby computing the upward iteration sequence

$$\bot = f^0(\bot) \sqsubseteq f^1(\bot) \sqsubseteq f^2(\bot) \sqsubseteq \cdots \sqsubseteq f^i(\bot) \sqsubseteq \cdots,$$

up to the first non-zero limit ordinal ω; namely,

$$\operatorname{lfp} f = f^\omega(\bot) \stackrel{\text{def}}{=} \bigsqcup_{i<\omega} f^i(\bot).$$

For each $f_0 \colon S_0 \to T_0$ and $f_1 \colon S_1 \to T_1$, the function $f_0[f_1] \colon (S_0 \cup S_1) \to (T_0 \cup T_1)$ is defined, for each $x \in S_0 \cup S_1$, by

$$\bigl(f_0[f_1]\bigr)(x) \stackrel{\text{def}}{=} \begin{cases} f_1(x), & \text{if } x \in S_1; \\ f_0(x), & \text{if } x \in S_0 \setminus S_1. \end{cases}$$

For $n > 0$, we denote by $\mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathbb{R}^n$ a n-tuple (vector) of real numbers; $\mathbb{R}_+$ is the set of non-negative real numbers; $\langle \mathbf{v}, \mathbf{w} \rangle$ denotes the scalar product of vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$; the vector $\mathbf{0} \in \mathbb{R}^n$ has all components equal to zero. We write $\mathbf{v} :: \mathbf{w}$ to denote the *tuple concatenation* of $\mathbf{v} \in \mathbb{R}^n$ and $\mathbf{w} \in \mathbb{R}^m$, so that $\mathbf{v} :: \mathbf{w} \in \mathbb{R}^{n+m}$.

Let $\mathbf{x}$ be a n-tuple of distinct variables. Then $\beta = \bigl(\langle \mathbf{a}, \mathbf{x} \rangle \bowtie b\bigr)$ denotes a linear inequality constraint, for each vector $\mathbf{a} \in \mathbb{R}^n$, where $\mathbf{a} \neq \mathbf{0}$, each scalar $b \in \mathbb{R}$, and $\bowtie \in \{\geq, >\}$. A linear inequality constraint β defines a (topologically closed or open) affine half-space of $\mathbb{R}^n$, denoted by $\operatorname{con}\bigl(\{\beta\}\bigr)$.

A set $\mathcal{P} \subseteq \mathbb{R}^n$ is a *(convex) polyhedron* if and only if $\mathcal{P}$ can be expressed as the intersection of a finite number of affine half-spaces of $\mathbb{R}^n$, i.e., as the solution $\mathcal{P} = \operatorname{con}(\mathcal{C})$ of a finite set of linear inequality constraints $\mathcal{C}$ (called a *constraint system*). The set of all polyhedra on the vector space $\mathbb{R}^n$ is denoted as $\mathbb{P}_n$. When partially ordered by set-inclusion, polyhedra form a lattice $(\mathbb{P}_n, \subseteq, \emptyset, \mathbb{R}^n, \uplus, \cap)$ having the empty set and $\mathbb{R}^n$ as the bottom and top element, respectively; the binary meet operation, returning the greatest polyhedron smaller than or equal to the two arguments, is easily seen to correspond to set-intersection; the binary join operation, returning the least polyhedron greater than or equal to the two arguments, is denoted '$\uplus$' and called *convex polyhedral hull* (poly-hull, for short). In general, the poly-hull of two polyhedra is different from their convex hull [SW70].

A relation $\psi \subseteq \mathbb{R}^n \times \mathbb{R}^n$ (of dimension n) is said to be *affine* if there exists $\ell \in \mathbb{N}$ and $\mathbf{a}_i, \mathbf{c}_i \in \mathbb{R}^n$, $b_i \in \mathbb{R}$ and $\bowtie_i \in \{\geq, >\}$, for each $i = 1, \ldots, \ell$, such that

$$\forall \mathbf{v}, \mathbf{w} \in \mathbb{R}^n : (\mathbf{v}, \mathbf{w}) \in \psi \iff \bigwedge_{i=1}^{\ell} \bigl(\langle \mathbf{c}_i, \mathbf{w} \rangle \bowtie_i \langle \mathbf{a}_i, \mathbf{v} \rangle + b_i\bigr).$$

Any affine relation of dimension n can thus be encoded by ℓ linear inequalities on a $2n$-tuple of distinct variables $\mathbf{x} :: \mathbf{x}'$ (playing the role of $\mathbf{v}$ and $\mathbf{w}$, respectively), therefore defining a polyhedron in $\mathbb{P}_{2n}$. The set of polyhedra $\mathbb{P}_n$ is closed under the (direct or inverse) application of affine relations: i.e., for each $\mathcal{P} \in \mathbb{P}_n$ and each affine relation $\psi \subseteq \mathbb{R}^n \times \mathbb{R}^n$, the image $\psi(\mathcal{P})$ and the preimage $\psi^{-1}(\mathcal{P})$ are in $\mathbb{P}_n$.

2.1. Abstract Interpretation. The semantics of a hardware or software system is a mathematical description of all its possible run-time behaviors. Different semantics can be defined for the same system, depending on the details being recorded. *Abstract interpretation* [CC77] is a formal method for relating these semantics according to their level of abstraction, so that questions about the behavior of a system can be provided with sound, possibly approximate answers.

The concrete semantics $c \in C$ of a program is usually formalized as the least fixpoint of a continuous semantic function $\mathcal{F} \colon C \to C$, where the concrete domain $(C, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$ is a complete lattice of semantic properties; in many interesting cases, the computational order '$\sqsubseteq$' corresponds to the approximation relation, so that $c_1 \sqsubseteq c_2$ holds if c_1 is a stronger property than c_2 (i.e., c_2 approximates c_1).

For instance, the run-time behavior of a program may be defined in terms of a transition system $\langle \Sigma, t, \iota \rangle$, where Σ is a set of states, $\iota \subseteq \Sigma$ is the subset of initial states, and $t \in \wp(\Sigma \times \Sigma)$ is a binary transition relation mapping a state to its possible successor states. Letting $\Sigma^\star$ denote the set of all finite sequences of elements in Σ, the initial history of a forward computation can be recorded[1] as a partial execution trace $\tau = \sigma_0 \cdots \sigma_m \in \Sigma^\star$ starting from an initial state $\sigma_0 \in \iota$ and such that any two consecutive states σ_i and σ_{i+1} are related by the transition relation, i.e., $(\sigma_i, \sigma_{i+1}) \in t$. In such a context, an element of the concrete domain $\bigl(\wp(\Sigma^\star), \subseteq, \emptyset, \Sigma^\star, \cup, \cap\bigr)$ is a set of partial execution traces and the concrete semantics is $\mathrm{lfp}(\mathcal{F})$, where the semantic function is defined by

$$\begin{aligned}\mathcal{F} = \lambda X \in \wp(\Sigma^\star) \,.\, X \cup \{\, \tau \in \Sigma^\star \mid \tau = \sigma_0 \in \iota \,\} \\ \cup \bigl\{\, \tau\sigma_{i+1} \in \Sigma^\star \bigm| \tau = \sigma_0 \cdots \sigma_i \in X, (\sigma_i, \sigma_{i+1}) \in t \,\bigr\}.\end{aligned}$$

An abstract domain[2] $(D^\sharp, \sqsubseteq, \bot, \sqcup)$ can be modeled as a bounded join-semilattice, so that it has a bottom element $\bot$ and the least upper bound $d_1^\sharp \sqcup d_2^\sharp$ exists for all $d_1^\sharp, d_2^\sharp \in D^\sharp$. This domain is related to the concrete domain by a monotonic and injective concretization function $\gamma \colon D^\sharp \to C$. Monotonicity and injectivity mean that the abstract partial order is equivalent to the approximation relation induced on $D^\sharp$ by the concretization function γ. Conversely, the concrete domain is related to the abstract one by a partial abstraction function $\alpha \colon C \rightarrowtail D^\sharp$ such that, for each $c \in C$, if $\alpha(c)$ is defined then $c \sqsubseteq \gamma\bigl(\alpha(c)\bigr)$. In particular, we assume that $\alpha(\bot) = \bot$ is always defined; when needed or useful, we will require a few additional properties.

For example, a first abstraction of the semantics above, typically adopted when discussing invariance properties of programs [CC79, CC92a], approximates a set of traces by the set of states occurring in any one of the traces. The *reachable states* are thus characterized by elements of the complete lattice $\bigl(\wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap\bigr)$, which plays here the role of the abstract domain. The concretization function relating $D^\sharp = \wp(\Sigma)$ to $C = \wp(\Sigma^\star)$ is defined, for each $d^\sharp \in \wp(\Sigma)$, by

$$\gamma(d^\sharp) \stackrel{\mathrm{def}}{=} \{\, \tau \in \Sigma^\star \mid \tau = \sigma_0 \cdots \sigma_m, \forall i = 0, \ldots, m : \sigma_i \in d^\sharp \,\}.$$

[1] This is just one of a wide range of possible semantics; by the same approach, other semantics may be described and related by abstract interpretation [CC92c].

[2] To avoid notational burden, whenever possible we will overload the lattice-theoretic symbols $\sqsubseteq$, $\bot$, $\sqcup$, etc., exploiting context to disambiguate their meaning.

Hence, the concrete semantic function $\mathcal{F}\colon \wp(\Sigma^\star) \to \wp(\Sigma^\star)$ can be approximated by the monotonic abstract semantic function $\mathcal{A}\colon \wp(\Sigma) \to \wp(\Sigma)$ defined by

$$\mathcal{A} = \lambda d^\sharp \in \wp(\Sigma) \,.\, d^\sharp \cup \iota \cup \bigl\{\, \sigma' \in \Sigma \bigm| \exists \sigma \in d^\sharp \,.\, (\sigma, \sigma') \in t \,\bigr\}.$$

This abstract semantic function is *sound* with respect to the concrete semantic function in that it satisfies the following local correctness requirement

$$\forall c \in C : \forall d^\sharp \in D^\sharp : c \sqsubseteq \gamma(d^\sharp) \implies \mathcal{F}(c) \sqsubseteq \gamma\bigl(\mathcal{A}(d^\sharp)\bigr),$$

ensuring that each iteration $\mathcal{F}^i(\bot)$ in the concrete fixpoint computation is safely approximated by computing the corresponding abstract iteration $\mathcal{A}^i\bigl(\alpha(\bot)\bigr)$. In particular, the least fixpoint of $\mathcal{F}$ is safely approximated by any post-fixpoint of $\mathcal{A}$ [CC77], i.e., any abstract element $d^\sharp \in D^\sharp$ such that $\mathcal{A}(d^\sharp) \sqsubseteq d^\sharp$.

Actually, the abstraction defined above satisfies an even stronger property, in that the abstract semantic function $\mathcal{A}$ is the *most precise* of all the sound approximations of $\mathcal{F}$ that could be defined on the considered abstract domain. This happens because the two domains are related by a Galois connection [CC77], i.e., there exists a total abstraction function $\alpha\colon C \to D^\sharp$ satisfying

$$\forall c \in C : \forall d^\sharp \in D^\sharp : \alpha(c) \sqsubseteq d^\sharp \iff c \sqsubseteq \gamma(d^\sharp).$$

Namely, for all $c \in \wp(\Sigma^\star)$, we can define

$$\alpha(c) \stackrel{\mathrm{def}}{=} \bigl\{\, \sigma_i \in \Sigma \bigm| \tau = \sigma_0 \cdots \sigma_m \in c, i \in \{0, \ldots, m\} \,\bigr\}.$$

For Galois connections it can be shown that $\alpha(c)$ is the best possible approximation in $D^\sharp$ for the concrete element $c \in C$; similarly, $\alpha \circ \mathcal{F} \circ \gamma$ (i.e., the function $\mathcal{A}$ defined above) is the best possible approximation for $\mathcal{F}$ [CC77, CC79]. Such a result is provided with a quite intuitive reading; in order to approximate the concrete function $\mathcal{F}$ on an abstract element $d^\sharp \in D^\sharp$: we first apply the concretization function γ so as to obtain the meaning of $d^\sharp$; then we apply the concrete function $\mathcal{F}$; finally, we abstract the result so as to obtain back an element of $D^\sharp$.

Abstract interpretation theory can thus be used to specify (semi-) automatic program analysis tools that are correct by design. Of course —due to well-known undecidability results— any fully automatic tool can only provide partial, though safe answers.

2.2. Abstract Domains for Boolean and Numeric Values. The reachable state abstraction described above is just one of the possible semantic approximations that can be adopted when specifying an abstract semantics. A further, typical approximation concerns the description of the states of the transition system. Each state $\sigma \in \Sigma$ may be decomposed into, e.g., a set of numerical or Boolean variables that are of interest for the application at hand; new abstract domains can be defined (and composed [CC79]) so as to soundly describe the possible values of these variables.

As an expository example that will be also used in the following sections, assume that part of a state is characterized by the value of an integer variable. Then, the domain $\bigl(\wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap\bigr)$ can be abstracted to the concrete domain of integers $\bigl(\wp(\mathrm{Int}), \subseteq, \emptyset, \mathrm{Int}, \cup, \cap\bigr)$. This domain is further approximated by an abstract domain $\bigl(\mathrm{Int}^\sharp, \sqsubseteq, \bot, \sqcup\bigr)$, via the concretization function $\gamma_{\mathrm{I}}\colon \mathrm{Int}^\sharp \to \wp(\mathrm{Int})$. Elements of $\mathrm{Int}^\sharp$ are denoted by $m^\sharp$, possibly subscripted. We assume that the partial abstraction function $\alpha_{\mathrm{I}}\colon \wp(\mathrm{Int}) \rightarrowtail \mathrm{Int}^\sharp$ is defined on all singletons $\{m\} \in \wp(\mathrm{Int})$ and on the whole set Int. We also assume that there are abstract binary operations '$\oplus$', '$\ominus$' and '$\circledast$' on $\mathrm{Int}^\sharp$ that are sound with respect to the corresponding operations on $\wp(\mathrm{Int})$ which, in turn, are the obvious pointwise extensions of addition, subtraction and multiplication over the integers. More formally, for '$\oplus$', we require soundness with respect to addition, i.e., $\gamma_{\mathrm{I}}(m_0^\sharp \oplus m_1^\sharp) \supseteq \bigl\{\, m_0 + m_1 \bigm| m_0 \in \gamma_{\mathrm{I}}(m_0^\sharp), m_1 \in \gamma_{\mathrm{I}}(m_1^\sharp) \,\bigr\}$, for each $m_0^\sharp, m_1^\sharp \in \mathrm{Int}^\sharp$. Similar requirements are imposed on '$\ominus$' and '$\circledast$'. Even though the definition of $\mathrm{Int}^\sharp$ is completely general, families of integer intervals come naturally to mind for this role.

Suppose now that some other part of the state is characterized by the value of a Boolean expression. Then, the domain $\bigl(\wp(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap\bigr)$ can be abstracted to the finite domain $\bigl(\wp(\mathrm{Bool}), \subseteq, \emptyset, \mathrm{Bool}, \cup, \cap\bigr)$, where $\mathrm{Bool} = \{\mathrm{ff}, \mathrm{tt}\}$ is the set of Boolean values. In general, such a finite domain may be further approximated by an abstract domain $(\mathrm{Bool}^\sharp, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$, related to the concrete domain by a Galois connection. Elements of $\mathrm{Bool}^\sharp$ are denoted by $t^\sharp$, possibly subscripted, and we can define abstract operations '$\oslash$', '$\circledvee$' and '$\circledwedge$' on $\mathrm{Bool}^\sharp$ that are sound with respect to the pointwise extensions of Boolean negation, disjunction and conjunction over $\wp(\mathrm{Bool})$. For instance, for the operation '$\circledvee$' to be sound with respect to disjunction on $\wp(\mathrm{Bool})$, it is required that, $\gamma_{\mathrm{B}}(t_0^\sharp \circledvee t_1^\sharp) \supseteq \bigl\{\, t_0 \vee t_1 \bigm| t_0 \in \gamma_{\mathrm{B}}(t_0^\sharp), t_1 \in \gamma_{\mathrm{B}}(t_1^\sharp) \,\bigr\}$ for each $t_0^\sharp$ and $t_1^\sharp$ in $\mathrm{Bool}^\sharp$. Likewise for '$\circledwedge$'. For '$\oslash$' the correctness requirement is that, for each $t^\sharp$ in $\mathrm{Bool}^\sharp$, $\gamma_{\mathrm{B}}(\oslash\, t^\sharp) \supseteq \bigl\{\, \neg t \bigm| t \in \gamma_{\mathrm{B}}(t^\sharp) \,\bigr\}$. Abstract comparison operations $\circledcirc, \otimes \colon \mathrm{Int}^\sharp \times \mathrm{Int}^\sharp \rightarrow \mathrm{Bool}^\sharp$ can then be defined to correctly approximate the equal-to and less-than tests: $\gamma_{\mathrm{B}}(m_0^\sharp \circledcirc m_1^\sharp) \supseteq \bigl\{\, m_0 = m_1 \bigm| m_0 \in \gamma_{\mathrm{I}}(m_0^\sharp), m_1 \in \gamma_{\mathrm{I}}(m_1^\sharp) \,\bigr\}$ for each $m_0^\sharp, m_1^\sharp \in \mathrm{Int}^\sharp$; likewise for '$\otimes$'.

Simple abstract domains such as the ones above can be combined in different ways so as to obtain quite accurate approximations [CC79]. In some cases, however, the required precision level may only be obtained by a suitable initial choice of the abstract domain. As a notable example, suppose that some part of the state $\sigma \in \Sigma$ is characterized by n (integer or real valued) numeric variables and the application at hand needs some *relational* information about these variables. In such a context, an approximation based on a simple conjunctive combination of n copies of the domain $\mathrm{Int}^\sharp$ described above will be almost useless. Rather, a new approximation scheme can be devised by modeling states using the domain $\bigl(\wp(\mathbb{R}^n), \subseteq, \emptyset, \mathbb{R}^n, \cup, \cap\bigr)$, where each vector $\mathbf{v} \in \mathbb{R}^n$ is meant to describe a possible valuation for the n variables. A further abstraction should map this domain so as to retain some of the relations holding between the values of the n variables. If a finite set of linear inequalities provides a good enough approximation, then the natural choice is to abstract this domain into the abstract domain of convex polyhedra $(\mathbb{P}_n, \subseteq, \emptyset, \mathbb{R}^n, \uplus, \cap)$ [CH78]. In this case, the concrete and abstract domain are not related by a Galois connection and hence, a best approximation might not exist.[3] Nonetheless, the convex polyhedral hull (partial) abstraction function $\uplus \colon \wp(\mathbb{R}^n) \rightarrowtail \mathbb{P}_n$ is defined in most of the cases of interest and provides the best possible approximation. Most of the arithmetic operations seen before can be encoded (or approximated) by computing images of affine relations.

[3]This happens, for instance, when approximating an n-dimensional ball with a convex polyhedron.

2.3. Widening Operators. It should be stressed that, in general, the abstract semantics described above is not finitely computable. For instance, both the domain of convex polyhedra and the domain of integer intervals have infinite ascending chains, so that the limit of a converging fixpoint computation cannot generally be reached in a finite number of iterations.

A finite computation can be enforced by further approximations resulting in a *Noetherian* abstract domain, i.e., a domain where all ascending chains are finite. Alternatively, and more generally, it is possible to keep an abstract domain with infinite chains, while enforcing that these chains are traversed in a finite number of iteration steps [CC92b]. In both cases, termination is usually achieved to the detriment of precision, so that an appropriate trade-off should be pursued. *Widening operators* [CC76, CC77, CC92a, CC92b] provide a simple and general characterization for the second option.

Definition 2.1. The partial operator $\nabla \colon D^\sharp \times D^\sharp \rightarrowtail D^\sharp$ is a *widening* if:

(1) for all $d^\sharp, e^\sharp \in D^\sharp$, $d^\sharp \sqsubseteq e^\sharp$ implies that $d^\sharp \mathbin{\nabla} e^\sharp$ is defined and $e^\sharp \sqsubseteq d^\sharp \mathbin{\nabla} e^\sharp$;
(2) for all increasing chains $e_0^\sharp \sqsubseteq e_1^\sharp \sqsubseteq \cdots$, the increasing chain defined by $d_0^\sharp \stackrel{\text{def}}{=} e_0^\sharp$ and $d_{i+1}^\sharp \stackrel{\text{def}}{=} d_i^\sharp \mathbin{\nabla} (d_i^\sharp \sqcup e_{i+1}^\sharp)$, for $i \in \mathbb{N}$, is not strictly increasing.

It can be proved that, for any monotonic operator $\mathcal{A} \colon D^\sharp \to D^\sharp$, the upward iteration sequence with widenings starting at the bottom element $d_0^\sharp \stackrel{\text{def}}{=} \bot$ and defined by

$$d_{i+1}^\sharp \stackrel{\text{def}}{=} \begin{cases} d_i^\sharp, & \text{if } \mathcal{A}(d_i^\sharp) \sqsubseteq d_i^\sharp, \\ d_i^\sharp \mathbin{\nabla} \bigl(d_i^\sharp \sqcup \mathcal{A}(d_i^\sharp)\bigr), & \text{otherwise,} \end{cases}$$

converges to a post-fixpoint of $\mathcal{A}$ after a finite number of iterations [CC92b]. Clearly, the choice of the widening has a deep impact on the precision of the results obtained. Designing a widening which is appropriate for a given application is therefore a difficult (but possibly rewarding) activity.

3. Analysis and Verification of Computer Programs

In this section we begin a review of the applications of polyhedral computations to analysis and verification problems starting with the the work of Cousot and Halbwachs [CH78, Hal79]. These seminal papers on the automatic inference of linear invariants for imperative programs constituted a major leap forward for at least two reasons. First, the polyhedral domain proposed by Cousot and Halbwachs was considerably more powerful than all the data-flow analyses known at that time, including the rather sophisticated one by Karr which was limited to linear equalities [Kar76, MS04]. Secondly, the use of convex polyhedra as an abstract domain established abstract interpretation as the right methodology for the definition of complex and correct program analyzers.

We illustrate the basic ideas by partially specifying the analysis of linear invariants for a very simple imperative language. The simplicity of the language we have chosen for expository purposes should not mislead the reader: the approach is generalizable to any imperative (and, for that matter, functional and logic) language [BHP+07]. The abstract syntax of the language is presented in Figure 1. The basic syntactic categories, corresponding to the sets Int, Bool and Var, are defined directly. From these, the categories of arithmetic and Boolean expressions and of

Integers: $m \in \mathrm{Int} \stackrel{\mathrm{def}}{=} \mathbb{Z}$
Booleans: $t \in \mathrm{Bool} \stackrel{\mathrm{def}}{=} \{\mathrm{tt}, \mathrm{ff}\}$
Variables: $x \in \mathrm{Var} \stackrel{\mathrm{def}}{=} \{x_0, x_1, x_2, \ldots\}$
Arithmetic expressions:

$$\mathrm{Aexp} \ni a ::= m \mid x \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 * a_1$$

Boolean expressions:

$$\mathrm{Bexp} \ni b ::= t \mid a_0 = a_1 \mid a_0 < a_1$$

Statements:

$$\mathrm{Stmt} \ni s ::= \mathbf{skip} \mid x := a \mid s_0; s_1 \mid \mathbf{if}\, e\, \mathbf{then}\, s_0\, \mathbf{else}\, s_1 \mid \mathbf{while}\, e\, \mathbf{do}\, s$$

FIGURE 1. Abstract syntax of the simple imperative language

statements are defined by means of BNF rules. Notice the use of syntactic meta-variables: for instance, to save typing we will consistently denote by s, possibly subscripted or superscripted, any element of Stmt.

The concrete semantics of programs is formally defined using the *natural semantics* approach [Kah87]. This, in turn, is a "big-step" operational semantics defined by structural induction on program structures in the style of Plotkin [Plo81]. First we define the notion of *store*, which is any mapping between a finite set of variables and elements of Int. Formally, stores are elements of the set

$$\mathrm{Store} \stackrel{\mathrm{def}}{=} \{\, \sigma \colon V \to \mathrm{Int} \mid V \subseteq_{\mathrm{f}} \mathrm{Var} \,\}$$

and will be denoted by the letter σ, possibly subscripted or superscripted. The store obtained from $\sigma \in \mathrm{Store}$ by the assignment of $m \in \mathrm{Int}$ to $x \in \mathrm{Var}$, denoted by $\sigma[m/x]$, is defined as follows, for each $x' \in \mathrm{Var}$:

$$\sigma[m/x](x') \stackrel{\mathrm{def}}{=} \begin{cases} m, & \text{if } x' = x; \\ \sigma(x'), & \text{if } x' \neq x. \end{cases}$$

The concrete evaluation relations that complete the definition of the concrete semantics for our simple language are defined by structural induction from a set of rule schemata. The evaluation relations for terminating computations are given by $\xrightarrow{\mathrm{a}} \subseteq (\mathrm{Aexp} \times \mathrm{Store}) \times \mathrm{Int}$, for arithmetic expressions, $\xrightarrow{\mathrm{b}} \subseteq (\mathrm{Bexp} \times \mathrm{Store}) \times \mathrm{Bool}$, for Boolean expressions, and $\xrightarrow{\mathrm{s}} \subseteq (\mathrm{Stmt} \times \mathrm{Store}) \times \mathrm{Store}$, for statements. The judgment $\langle a, \sigma \rangle \xrightarrow{\mathrm{a}} m$ means that when expression a is executed in store σ it results in the integer m. The judgment $\langle b, \sigma \rangle \xrightarrow{\mathrm{b}} t$ is similar. Note that expressions do not have, in our simple language, side effects. The judgment $\langle s, \sigma \rangle \xrightarrow{\mathrm{s}} \sigma'$ means that the statement s, executed in store σ, results in a (possibly modified) store σ'. The rule schemata, in the form $\frac{\text{premise}}{\text{conclusion}}$, that define these relations are given in Figure 2. Rule instances can be composed in the obvious way to form finite tree structures, representing finite computations. Figure 3 shows one such tree.

The possibly infinite set of all finite trees is obtained by means of a least fixpoint computation, corresponding to the classical inductive interpretation of the rules in Figure 2. The rule schemata in Figure 4 can be used to directly model non-terminating computations and need to be interpreted coinductively

$$\frac{}{\langle m, \sigma\rangle \xrightarrow{\mathrm{a}} m} \qquad \frac{}{\langle x, \sigma\rangle \xrightarrow{\mathrm{a}} \sigma(x)} \qquad \frac{\langle a_0, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 \quad \langle a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_1}{\langle a_0 + a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 + m_1}$$

$$\frac{\langle a_0, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 \quad \langle a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_1}{\langle a_0 - a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 - m_1} \qquad \frac{\langle a_0, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 \quad \langle a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_1}{\langle a_0 * a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 \cdot m_1}$$

$$\frac{\langle a_0, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 \quad \langle a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_1}{\langle a_0 = a_1, \sigma\rangle \xrightarrow{\mathrm{b}} (m_0 = m_1)} \qquad \frac{\langle a_0, \sigma\rangle \xrightarrow{\mathrm{a}} m_0 \quad \langle a_1, \sigma\rangle \xrightarrow{\mathrm{a}} m_1}{\langle a_0 < a_1, \sigma\rangle \xrightarrow{\mathrm{b}} (m_0 < m_1)}$$

$$\frac{}{\langle \mathbf{skip}, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma} \qquad \frac{\langle a, \sigma\rangle \xrightarrow{\mathrm{a}} m}{\langle x := a, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma[m/x]} \qquad \frac{\langle s_0, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'' \quad \langle s_1, \sigma''\rangle \xrightarrow{\mathrm{s}} \sigma'}{\langle s_0; s_1, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'}$$

$$\frac{\langle b, \sigma\rangle \xrightarrow{\mathrm{b}} \mathrm{tt} \quad \langle s_0, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'}{\langle \mathbf{if}\, b\, \mathbf{then}\, s_0\, \mathbf{else}\, s_1, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'} \qquad \frac{\langle b, \sigma\rangle \xrightarrow{\mathrm{b}} \mathrm{ff} \quad \langle s_1, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'}{\langle \mathbf{if}\, b\, \mathbf{then}\, s_0\, \mathbf{else}\, s_1, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'}$$

$$\frac{\langle b, \sigma\rangle \xrightarrow{\mathrm{b}} \mathrm{ff}}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma} \qquad \frac{\langle b, \sigma\rangle \xrightarrow{\mathrm{b}} \mathrm{tt} \quad \langle c, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'' \quad \langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma''\rangle \xrightarrow{\mathrm{s}} \sigma'}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma\rangle \xrightarrow{\mathrm{s}} \sigma'}$$

FIGURE 2. Concrete semantics rule schemata for the finite computations of the simple imperative language

[CC92c, Ler06, Sch98]. The judgment $\langle s, \sigma\rangle \xrightarrow{\infty}$ means that the statement s diverges when executed in store σ. By a suitable adaptation of the computational ordering, both sets of finite and infinite trees can be jointly computed in a single least fixpoint computation [CC92c, Ler06, Sch98]. While these semantics characterizations contain all the information we need to perform a wide range of program reasoning tasks, they are generally not computable: we have thus to resort to approximation.

Following the abstract interpretation approach, as instantiated in [Sch95, Sch97, Sch98], the concrete rule schemata are paired with abstract rule schemata that correctly approximate them. Before doing that, we need to formalize abstract domains for each concrete domain used by the concrete semantics.

For simple approximations of integers and Boolean expressions, we consider the abstract domains $\mathrm{Int}^\sharp$ and $\mathrm{Bool}^\sharp$ introduced in Section 2.2. The last (and most interesting) abstraction we need is for approximating sets of stores. We thus require an abstract domain $\bigl(\mathrm{Store}^\sharp, \sqsubseteq, \bot, \sqcup\bigr)$ that is related, by means of a concretization function γ_{S} such that $\gamma_{\mathrm{S}}(\bot) = \emptyset$, to the concrete domain $\bigl(\wp(\mathrm{Store}), \subseteq, \emptyset, \mathrm{Store}, \cup, \cap\bigr)$. Elements of $\mathrm{Store}^\sharp$ are denoted by $\sigma^\sharp$, possibly subscripted. The abstract store evaluation and update operators

$$\cdot[\cdot] \colon (\mathrm{Store}^\sharp \times \mathrm{Aexp}) \to \mathrm{Int}^\sharp,$$
$$\cdot[\cdot := \cdot] \colon \bigl(\mathrm{Store}^\sharp \times \mathrm{Var} \times \mathrm{Aexp}\bigr) \to \mathrm{Store}^\sharp,$$
$$\cdot[\cdot/\cdot] \colon \bigl(\mathrm{Store}^\sharp \times \mathrm{Var} \times \mathrm{Int}^\sharp\bigr) \to \mathrm{Store}^\sharp$$

$$
\dfrac{
\dfrac{\dfrac{}{\langle 0, \sigma_0\rangle \xrightarrow{\mathrm{a}} 0} \quad \dfrac{}{\langle x_0, \sigma_0\rangle \xrightarrow{\mathrm{a}} 1}}{\langle 0 < x_0, \sigma_0\rangle \xrightarrow{\mathrm{b}} \mathrm{tt}}
\quad
\dfrac{
\dfrac{\dfrac{\dfrac{}{\langle x_1, \sigma_0\rangle \xrightarrow{\mathrm{a}} 1} \quad \dfrac{}{\langle 2, \sigma_0\rangle \xrightarrow{\mathrm{a}} 2}}{\langle x_1 + 2, \sigma_0\rangle \xrightarrow{\mathrm{a}} 3}}{\langle x_1 := x_1 + 2, \sigma_0\rangle \xrightarrow{\mathrm{s}} \sigma_1}
\quad
\dfrac{\dfrac{\dfrac{}{\langle x_0, \sigma_1\rangle \xrightarrow{\mathrm{a}} 1} \quad \dfrac{}{\langle x_1, \sigma_1\rangle \xrightarrow{\mathrm{a}} 3}}{\langle x_0 - x_1, \sigma_1\rangle \xrightarrow{\mathrm{a}} -2}}{\langle x_0 := x_0 - x_1, \sigma_1\rangle \xrightarrow{\mathrm{s}} \sigma_2}
}{\big\langle (x_1 := x_1 + 2; x_0 := x_0 - x_1), \sigma_0\big\rangle \xrightarrow{\mathrm{s}} \sigma_2}
\quad
\dfrac{\dfrac{\dfrac{}{\langle 0, \sigma_2\rangle \xrightarrow{\mathrm{a}} 0} \quad \dfrac{}{\langle x_0, \sigma_2\rangle \xrightarrow{\mathrm{a}} -2}}{\langle 0 < x_0, \sigma_2\rangle \xrightarrow{\mathrm{b}} \mathrm{ff}}}{\langle w, \sigma_2\rangle \xrightarrow{\mathrm{s}} \sigma_2}
}{\big\langle \mathbf{while}\ 0 < x_0\ \mathbf{do}\,(x_1 := x_1 + 2; x_0 := x_0 - x_1), \sigma_0\big\rangle \xrightarrow{\mathrm{s}} \sigma_2}
$$

Legend:

$$\sigma_0 \stackrel{\mathrm{def}}{=} \big\{(x_0, 1), (x_1, 1)\big\},$$

$$\sigma_1 \stackrel{\mathrm{def}}{=} \big\{(x_0, 1), (x_1, 3)\big\},$$

$$\sigma_2 \stackrel{\mathrm{def}}{=} \big\{(x_0, -2), (x_1, 3)\big\},$$

$$w \stackrel{\mathrm{def}}{=} \big(\mathbf{while}\ 0 < x_0\ \mathbf{do}\,(x_1 := x_1 + 2; x_0 := x_0 - x_1)\big).$$

FIGURE 3. The tree representing a concrete execution of a program

$$\frac{\langle s_0, \sigma\rangle \overset{\infty}{\rightarrow}}{\langle s_0; s_1, \sigma\rangle \overset{\infty}{\rightarrow}} \qquad \frac{\langle s_0, \sigma\rangle \overset{\mathrm{s}}{\rightarrow} \sigma' \quad \langle s_1, \sigma'\rangle \overset{\infty}{\rightarrow}}{\langle s_0; s_1, \sigma\rangle \overset{\infty}{\rightarrow}}$$

$$\frac{\langle b, \sigma\rangle \overset{\mathrm{b}}{\rightarrow} \mathrm{tt} \quad \langle s_0, \sigma\rangle \overset{\infty}{\rightarrow}}{\langle \mathbf{if}\, b\, \mathbf{then}\, s_0\, \mathbf{else}\, s_1, \sigma\rangle \overset{\infty}{\rightarrow}} \qquad \frac{\langle b, \sigma\rangle \overset{\mathrm{b}}{\rightarrow} \mathrm{ff} \quad \langle s_1, \sigma\rangle \overset{\infty}{\rightarrow}}{\langle \mathbf{if}\, b\, \mathbf{then}\, s_0\, \mathbf{else}\, s_1, \sigma\rangle \overset{\infty}{\rightarrow}}$$

$$\frac{\langle b, \sigma\rangle \overset{\mathrm{b}}{\rightarrow} \mathrm{tt} \quad \langle c, \sigma\rangle \overset{\infty}{\rightarrow}}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma\rangle \overset{\infty}{\rightarrow}} \qquad \frac{\langle b, \sigma\rangle \overset{\mathrm{b}}{\rightarrow} \mathrm{tt} \quad \langle c, \sigma\rangle \overset{\mathrm{s}}{\rightarrow} \sigma' \quad \langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma'\rangle \overset{\infty}{\rightarrow}}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma\rangle \overset{\infty}{\rightarrow}}$$

FIGURE 4. Additional concrete semantics rule schemata for the infinite computations of the simple imperative language

are assumed to be sound with respect to their concrete counterparts, i.e., such that, for each $\sigma^\sharp \in \mathrm{Store}^\sharp$, $a \in \mathrm{Aexp}$, $x \in \mathrm{Var}$ and $m^\sharp \in \mathrm{Int}^\sharp$:

$$\begin{aligned} \gamma_{\mathrm{I}}\bigl(\sigma^\sharp[a]\bigr) &\supseteq \bigl\{\, m \in \mathrm{Int} \bigm| \sigma \in \gamma_{\mathrm{S}}(\sigma^\sharp), \langle a, \sigma\rangle \overset{\mathrm{a}}{\rightarrow} m \,\bigr\}, \\ \gamma_{\mathrm{S}}\bigl(\sigma^\sharp[x := a]\bigr) &\supseteq \bigl\{\, \sigma' \in \mathrm{Store} \bigm| \sigma \in \gamma_{\mathrm{S}}(\sigma^\sharp), \langle x := a, \sigma\rangle \overset{\mathrm{s}}{\rightarrow} \sigma' \,\bigr\}, \\ \gamma_{\mathrm{S}}\bigl(\sigma^\sharp[m^\sharp/x]\bigr) &\supseteq \bigl\{\, \sigma[m/x] \in \mathrm{Store} \bigm| \sigma \in \gamma_{\mathrm{S}}(\sigma^\sharp), m \in \gamma_{\mathrm{I}}(m^\sharp) \,\bigr\}. \end{aligned}$$

We also need computable "Boolean filters" to refine the information contained in abstract stores. These are given by two functions $\phi_{\mathrm{tt}}, \phi_{\mathrm{ff}} \colon \mathrm{Store}^\sharp \times \mathrm{Bexp} \rightarrow \mathrm{Store}^\sharp$ such that, for each $\sigma^\sharp \in \mathrm{Store}^\sharp$ and $b \in \mathrm{Bexp}$:

$$\begin{aligned} \gamma_{\mathrm{S}}\bigl(\phi_{\mathrm{tt}}(\sigma^\sharp, b)\bigr) &\supseteq \bigl\{\, \sigma \in \gamma_{\mathrm{S}}(\sigma^\sharp) \bigm| \langle b, \sigma\rangle \overset{\mathrm{b}}{\rightarrow} \mathrm{tt} \,\bigr\}, \\ \gamma_{\mathrm{S}}\bigl(\phi_{\mathrm{ff}}(\sigma^\sharp, b)\bigr) &\supseteq \bigl\{\, \sigma \in \gamma_{\mathrm{S}}(\sigma^\sharp) \bigm| \langle b, \sigma\rangle \overset{\mathrm{b}}{\rightarrow} \mathrm{ff} \,\bigr\}. \end{aligned}$$

We are now in a position to present, in Figure 5, a possible set of domain-independent abstract rules schemata. These schemata allow for the free approximation of the '$\rightsquigarrow$' right-hand sides in the conclusions. This means that if, e.g.,

$$\frac{\text{premise}}{\langle s, \sigma\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_1^\sharp}$$

is an instance of some rule, then

$$\frac{\text{premise}}{\langle s, \sigma\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_2^\sharp}$$

is also an instance of the same rule for each $\sigma_2^\sharp$ such that $\sigma_1^\sharp \sqsubseteq \sigma_2^\sharp$. Hence the schemata in Figure 5 ensure correctness yet leaving complete freedom about precision. The ability to give up some precision, as we will see, is crucial in order to ensure the (reasonably quick) termination of the analysis.

It is possible to prove that, for each (possibly infinite) concrete tree T built using the schemata of Figures 2 and 4, for each (possibly infinite) abstract tree $T^\sharp$ built using the schemata of Figure 5, if the concrete tree root is of the form $\langle s, \sigma\rangle \overset{\mathrm{s}}{\rightarrow} \sigma_1$ (when the tree is finite) or $\langle s, \sigma\rangle \overset{\infty}{\rightarrow}$ (when the tree is infinite) and the abstract tree root is of the form $\langle s, \sigma^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_1^\sharp$ with $\sigma \in \gamma_{\mathrm{S}}(\sigma^\sharp)$, then $T^\sharp$ correctly approximates T. This means not only that $\sigma_1 \in \gamma_{\mathrm{S}}(\sigma_1^\sharp)$ (when T is finite), but also that *each* node in T is correctly approximated by at least one node in $T^\sharp$. In other

$$\frac{}{\langle m, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} \alpha_{\mathrm{I}}\bigl(\{m\}\bigr)} \qquad \frac{}{\langle x, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} \sigma^\sharp[x]} \qquad \frac{\langle a_0, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \quad \langle a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_1^\sharp}{\langle a_0 + a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \oplus m_1^\sharp}$$

$$\frac{\langle a_0, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \quad \langle a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_1^\sharp}{\langle a_0 - a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \ominus m_1^\sharp} \qquad \frac{\langle a_0, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \quad \langle a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_1^\sharp}{\langle a_0 * a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \circledast m_1^\sharp}$$

$$\frac{}{\langle t, \sigma^\sharp\rangle \overset{\mathrm{b}}{\rightsquigarrow} \alpha_{\mathrm{B}}\bigl(\{t\}\bigr)} \qquad \frac{\langle a_0, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \quad \langle a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_1^\sharp}{\langle a_0 = a_1, \sigma^\sharp\rangle \overset{\mathrm{b}}{\rightsquigarrow} m_0^\sharp \circledcirc m_1^\sharp}$$

$$\frac{\langle a_0, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_0^\sharp \quad \langle a_1, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m_1^\sharp}{\langle a_0 < a_1, \sigma^\sharp\rangle \overset{\mathrm{b}}{\rightsquigarrow} m_0^\sharp \otimes m_1^\sharp} \qquad \frac{}{\langle \mathbf{skip}, \sigma^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma^\sharp}$$

$$\frac{\langle a, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m^\sharp}{\langle x := a, \sigma^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma^\sharp[x := a]}\ \text{(i)} \qquad \frac{\langle a, \sigma^\sharp\rangle \overset{\mathrm{a}}{\rightsquigarrow} m^\sharp}{\langle x := a, \sigma^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma^\sharp[m^\sharp/x]}\ \text{(ii)}$$

$$\frac{\langle s_0, \sigma_0^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_1^\sharp \quad \langle s_1, \sigma_1^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_2^\sharp}{\langle s_0; s_1, \sigma_0^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_2^\sharp}$$

$$\frac{\langle b, \sigma^\sharp\rangle \overset{\mathrm{b}}{\rightsquigarrow} t^\sharp \quad \bigl\langle s_0, \phi_{\mathrm{tt}}(\sigma^\sharp, b)\bigr\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_0^\sharp \quad \bigl\langle s_1, \phi_{\mathrm{ff}}(\sigma^\sharp, b)\bigr\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_1^\sharp}{\langle \mathbf{if}\, b\, \mathbf{then}\, s_0\, \mathbf{else}\, s_1, \sigma^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_0^\sharp \sqcup \sigma_1^\sharp}$$

$$\frac{\langle b, \sigma^\sharp\rangle \overset{\mathrm{b}}{\rightsquigarrow} t^\sharp \quad \bigl\langle c, \phi_{\mathrm{tt}}(\sigma^\sharp, b)\bigr\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_1^\sharp \quad \langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma_1^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \sigma_2^\sharp}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma^\sharp\rangle \overset{\mathrm{s}}{\rightsquigarrow} \phi_{\mathrm{ff}}(\sigma^\sharp, b) \sqcup \sigma_2^\sharp}$$

Notes:

(i) This rule is used if the domain $\mathrm{Store}^\sharp$ can capture the assignment precisely (e.g., when $\mathrm{Store}^\sharp$ is a domain of convex polyhedra and a is an affine expression). Notice that the premise is intentionally not used: its presence is required in order to ensure that the abstract tree approximates the concrete tree in its entirety.

(ii) This rule is used when (i) is not applicable.

FIGURE 5. Abstract semantics rule schemata for the simple imperative language

words, the abstract tree correctly approximates the entire concrete computation (see [BHP+07] for the details).

It is worth stressing the observation in [Sch98] that, even when disregarding the non-terminating concrete computations, the abstract rules still have to be interpreted coinductively because most of the finite concrete trees can only be approximated by infinite abstract trees; for instance, all abstract trees containing a while loop are infinite. Since, in general, we cannot effectively compute infinite abstract trees, we still do not have a viable analysis technique. The solution is to restrict ourselves to the class of rational trees, i.e., trees with only finitely many subtrees and that, consequently, admit a finite representation.

The analysis algorithm is sketched in [Sch95]. For expository purposes, we describe here a simplified version that is enough to handle the considered programming language features. The algorithm works by recursively constructing a finite approximation for the (possibly infinite) abstract subtree rooted in the current node (initially, the root of the whole tree). The current node $n = \bigl(\langle p, \sigma_n^\sharp \rangle \rightsquigarrow r_n\bigr)$, where r_n is a placeholder for the "yet to be computed" conclusion, is processed according to the following alternatives.

(1) If no ancestor of n has p in the label, the node has to be expanded using an applicable abstract rule instance. Namely, descendants of the premises of the rule are (recursively) processed, one at a time and from left to right. When the expansion of all the premises has been completed, including the case when the rule has no premise at all, the marker r_n is replaced by an abstract value computed according to the conclusion of the rule;
(2) If there exists an ancestor node $m = \langle p, \sigma_m^\sharp \rangle \rightsquigarrow r_m$ of n labeled by the same syntax p and such that $\sigma_n^\sharp \sqsubseteq \sigma_m^\sharp$, i.e., if node n is subsumed by node m, then the node is not expanded further and the placeholder r_n is replaced by the least fixpoint of the equation $r_n = f_m(r_n)$, where f_m is the expression corresponding to the conclusion of the abstract rule that was used for the expansion of node m;[4]
(3) Otherwise, there must be an ancestor node $m = \langle p, \sigma_m^\sharp \rangle \rightsquigarrow r_m$ of n labeled by the same syntax p, but the subsumption condition $\sigma_n^\sharp \sqsubseteq \sigma_m^\sharp$ does not hold. Then there are two options:
    (a) if the abstract domain $\mathrm{Store}^\sharp$ is finite, we proceed as in case (1);
    (b) if the abstract domain $\mathrm{Store}^\sharp$ is infinite, to ensure convergence, a widening '∇' over $\mathrm{Store}^\sharp$ can be employed[5] and store $\sigma_n^\sharp$ in node n is replaced by $\sigma_m^\sharp \mathbin{\nabla} (\sigma_m^\sharp \sqcup \sigma_n^\sharp)$. Then, we proceed again as in case (1).

The abstract semantics of Figure 5 and the given algorithm for computing a rational abstract tree are fully generic in that any choice for the abstract domains $\mathrm{Int}^\sharp$, $\mathrm{Bool}^\sharp$ and $\mathrm{Store}^\sharp$ will result into a provably correct analysis algorithm. Focusing on numerical domains, the role of $\mathrm{Int}^\sharp$ can be played by any domain of intervals, so that the operations '$\oplus$', '$\ominus$' and '$\circledast$' are the standard ones of interval arithmetic [AH83]; for instance, $[m_0^{\mathrm{l}}, m_0^{\mathrm{u}}] \oplus [m_1^{\mathrm{l}}, m_1^{\mathrm{u}}] \stackrel{\mathrm{def}}{=} [m_0^{\mathrm{l}} + m_1^{\mathrm{l}}, m_0^{\mathrm{u}} + m_1^{\mathrm{u}}]$. More sophisticated domains, such as *modulo intervals* [NJPF99], are able to encode more precise information about the set of *integer* values each variable can take. For $\mathrm{Store}^\sharp$, a common choice is to abstract from the integrality of variables and consider a domain of convex polyhedra which, in exchange, allows the tracking of relational information. With reference to Figure 5, rule (i) can be applied directly when the arithmetic expression $a = \langle \mathbf{a}, \mathbf{x} \rangle + b$ is affine; the corresponding polyhedral operation is the computation of the image of a polyhedron by a special case of affine

[4] As explained in [Sch95, Sch98], the computation of such a *least* fixpoint (in the context of a coinductive interpretation of the abstract rules) is justified by the fact that here we only need to approximate the conclusions produced by the terminating concrete computations, i.e., by the concrete rules of Figure 2, which are interpreted inductively. Also note that the divergence rules of Figure 4 have no conclusion at all.

[5] If $\mathrm{Store}^\sharp$ is infinite but Noetherian, we can choose $\nabla \stackrel{\mathrm{def}}{=} \sqcup$ as a widening.

relation $\psi \subseteq \mathbb{R}^n \times \mathbb{R}^n$, called *single-update affine function*:

$$(\mathbf{v}, \mathbf{w}) \in \psi \iff w_k = \langle \mathbf{a}, \mathbf{v} \rangle + b \wedge \bigwedge_{\substack{0 \leq i < n \\ i \neq k}} w_i = v_i.$$

Another special case, slightly more general than the one above and called *single-update bounded affine relation*, allows among other things to approximate nonlinear assignments and to realize rule (ii). For fixed vectors $\mathbf{a}, \mathbf{c} \in \mathbb{R}^n$ and scalars $b, d \in \mathbb{R}$:

$$(\mathbf{v}, \mathbf{w}) \in \psi \iff \langle \mathbf{a}, \mathbf{v} \rangle + b \leq w_k \leq \langle \mathbf{c}, \mathbf{v} \rangle + d \wedge \bigwedge_{\substack{0 \leq i < n \\ i \neq k}} w_i = v_i.$$

Both the rules for the if-then-else and the while constructs require the Boolean filters and least upper bound operations: these are realized by means of intersections (or the addition of individual constraints) and poly-hulls, respectively. These, together with the containment test used to detect the reaching of post-fixpoints and the widening (see Section 7) required to ensure termination of the analysis algorithm, are all the operations required for the analysis of our simple imperative language. More complex languages require other operations: for instance, the analysis of languages with command blocks require the possibility of embedding polyhedra into a space of higher dimension, reorganizing the dimensions, and projecting polyhedra on spaces of lower dimension. Other operations are needed to accommodate different semantic constructions (e.g., affine preimages for backward semantics), to allow for the efficient modeling of data objects (e.g., summarized dimensions to approximate the values of unbounded collections [GRS05]), and to help scalability (e.g., simplifications of polyhedra [Fre05]).

Figure 6 illustrates an abstract computation that, by following the algorithm above, approximates the concrete tree in Figure 3: intervals and polyhedra approximate sets of integers and sets of stores, respectively. The initial abstract store is given by the polyhedron $\mathcal{P}_0 = \operatorname{con}\bigl(\{x_0 \geq 1, x_1 = 1\}\bigr)$, which approximates all concrete stores σ satisfying $\sigma(x_0) \geq 1$ and $\sigma(x_1) = 1$ including the concrete store σ_0 in Figure 3. Consider first the lower tree in Figure 3. This corresponds to the stage in the computation when all possible instances of case (1) of the algorithm have been applied. In particular, the two leftmost subtrees are derived according to the abstract semantics rules in Figure 5 by only using case (1) of the algorithm. For the rightmost child which has still to be expanded, $\mathcal{P}$ is a placeholder for its conclusion. It is also noted that, in the root of this tree, since $\mathcal{P}_0^f = \emptyset$, the final result will be the same as the value assigned to $\mathcal{P}$. Since the rightmost child, satisfies the conditions of case (3b) of the algorithm, the abstract store $\mathcal{P}_1$ must undergo a widening computation, yielding the abstract store $\mathcal{Q}_0$. Thus this node has to be replaced by $\langle w, \mathcal{Q}_0 \rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P}$. Consider now the upper tree in Figure 3 which has the root $\langle w, \mathcal{Q}_0 \rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P}$ as above. The two left-most immediate subtrees are derived, as in the lower tree, by only using case (1) of the algorithm. The rightmost child is initially given $\mathcal{Q}$ as a placeholder for its conclusion. Since this node satisfies the conditions for case (2) of the algorithm, it is not expanded further; and the value of $\mathcal{Q}$ is obtained by finding the least fixpoint solution for the equation $\mathcal{Q} = \mathcal{Q}_0^f \uplus \mathcal{Q}$; namely, $\mathcal{Q}_0^f = \operatorname{con}\bigl(\{2x_0 + 3x_1 \geq 5, x_0 \leq 0\}\bigr)$. Thus in the conclusion of the root of the upper tree we have $\mathcal{P} = \mathcal{Q}_0^f \uplus \mathcal{Q} = \mathcal{Q}_0^f$. Finally, the completed abstract tree

$$
\dfrac{
\dfrac{\overline{\langle 0, \mathcal{Q}_0\rangle \overset{\mathrm{a}}{\rightsquigarrow} [0,0]} \quad \overline{\langle x_0, \mathcal{Q}_0\rangle \overset{\mathrm{a}}{\rightsquigarrow} \top}}{\langle 0 < x_0, \mathcal{Q}_0\rangle \overset{\mathrm{b}}{\rightsquigarrow} \top}
\quad
\dfrac{\dfrac{[\cdots]}{\langle x_1 := x_1 + 2, \mathcal{Q}_0^t\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{Q}_0'}\ \text{(i)} \quad \dfrac{[\cdots]}{\langle x_0 := x_0 - x_1, \mathcal{Q}_0'\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{Q}_1}\ \text{(i)}}{\big\langle (x_1 := x_1 + 2;\ x_0 := x_0 - x_1), \mathcal{Q}_0^t\big\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{Q}_1}
\quad
\overline{\langle w, \mathcal{Q}_1\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{Q} = \mathcal{Q}_0^f}\ (2)
}{
\langle w, \mathcal{Q}_0\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P} = (\mathcal{Q}_0^f \uplus \mathcal{Q}) = \mathcal{Q}_0^f\ (2)
}
$$

$$
\dfrac{
\dfrac{\overline{\langle 0, \mathcal{P}_0\rangle \overset{\mathrm{a}}{\rightsquigarrow} [0,0]} \quad \overline{\langle x_0, \mathcal{P}_0\rangle \overset{\mathrm{a}}{\rightsquigarrow} [1,\infty]}}{\langle 0 < x_0, \mathcal{P}_0\rangle \overset{\mathrm{b}}{\rightsquigarrow} \alpha_{\mathrm{B}}\big(\{\mathrm{tt}\}\big)}
\quad
\dfrac{\dfrac{[\cdots]}{\langle x_1 := x_1 + 2, \mathcal{P}_0^t\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P}_0'}\ \text{(i)} \quad \dfrac{[\cdots]}{\langle x_0 := x_0 - x_1, \mathcal{P}_0'\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P}_1}\ \text{(i)}}{\big\langle (x_1 := x_1 + 2;\ x_0 := x_0 - x_1), \mathcal{P}_0^t\big\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P}_1}
\quad
\langle w, \mathcal{P}_1\rangle \overset{\mathrm{s}}{\rightsquigarrow} \mathcal{P}\ \text{(3b)}
}{
\langle w, \mathcal{P}_0\rangle \overset{\mathrm{s}}{\rightsquigarrow} (\mathcal{P}_0^f \uplus \mathcal{P}) = (\emptyset \uplus \mathcal{P}) = \mathcal{P}
}
$$

Legend:

$$w \stackrel{\mathrm{def}}{=} \big(\textbf{while } 0 < x_0 \textbf{ do } (x_1 := x_1 + 2;\ x_0 := x_0 - x_1)\big),$$

$$\mathcal{P}_0 \stackrel{\mathrm{def}}{=} \mathrm{con}\big(\{x_0 \geq 1, x_1 = 1\}\big), \qquad \mathcal{Q}_0 \stackrel{\mathrm{def}}{=} \mathcal{P}_0 \mathbin{\nabla} (\mathcal{P}_0 \uplus \mathcal{P}_1) = \mathrm{con}\big(\{2x_0 + 3x_1 \geq 5, x_1 \geq 1\}\big),$$

$$\mathcal{P}_0^t \stackrel{\mathrm{def}}{=} \phi_{\mathrm{tt}}(\mathcal{P}_0, 0 < x_0) = \mathcal{P}_0, \qquad \mathcal{Q}_0^t \stackrel{\mathrm{def}}{=} \phi_{\mathrm{tt}}(\mathcal{Q}_0, 0 < x_0) = \mathrm{con}\big(\{x_0 \geq 1, x_1 \geq 1\}\big),$$

$$\mathcal{P}_0^f \stackrel{\mathrm{def}}{=} \phi_{\mathrm{ff}}(\mathcal{P}_0, 0 < x_0) = \emptyset, \qquad \mathcal{Q}_0^f \stackrel{\mathrm{def}}{=} \phi_{\mathrm{ff}}(\mathcal{Q}_0, 0 < x_0) = \mathrm{con}\big(\{2x_0 + 3x_1 \geq 5, x_0 \leq 0\}\big),$$

$$\mathcal{P}_0' \stackrel{\mathrm{def}}{=} \mathrm{con}\big(\{x_0 \geq 1, x_1 = 3\}\big), \qquad \mathcal{Q}_0' \stackrel{\mathrm{def}}{=} \mathrm{con}\big(\{x_0 \geq 1, x_1 \geq 3\}\big),$$

$$\mathcal{P}_1 \stackrel{\mathrm{def}}{=} \mathrm{con}\big(\{x_0 \geq -2, x_1 = 3\}\big), \qquad \mathcal{Q}_1 \stackrel{\mathrm{def}}{=} \mathrm{con}\big(\{x_0 + x_1 \geq 1, x_1 \geq 3\}\big).$$

Notes:

(i) Rule (i) of Figure 5 is used here.
(2) Case (2) of the algorithm is applied here.
(3b) Case (3b) of the algorithm is applied here.

FIGURE 6. Finite approximation of an infinite abstract computation tree

can be obtained by replacing the rightmost child of the lower tree by the upper tree and the placeholder $\mathcal{P}$ in the conclusion of the root of the lower tree by $\mathcal{Q}_0^f$.

Based on suitable variations of the simple linear invariant analysis outlined in this section (possibly combined with other analyses), many different applications have been proposed in the literature. Examples include the absence of common run-time arithmetic errors, such as floating-point exceptions, overflows and divisions by zero [BCC+03]; the absence of out-of-bounds array indexing [CH78, VB04], as well as other buffer overruns caused by incorrect string manipulations [DRS01, Ell04]; the analysis of programs manipulating (possibly unbounded) heap-allocated data structures, so as to prove the absence of several kinds of pointer errors (e.g., memory leaks) [GRS05, SKS00]; the detection of potential security vulnerabilities in x86 binaries that allow to bypass intrusion detection systems [KKM+05]; the inference of temporal schedulability constraints that a partially specified set of real-time tasks has to satisfy [DM05]. All of the above are examples of *safety* properties, whereby a computer program is proved to be free from some undesired behavior. However, the computation of invariant linear relations is also an important, often indispensable step when aiming at proving *progress* properties, such as termination [Cou05, MB05, SV91]. It should be also stressed that the same approach, after some minor adaptations, can be applied to the analysis of alternative computation paradigms such as, e.g., *gated data dependence graphs* [HU04] (an intermediate representation for compilers) and *batch workflow networks* [vOSV06] (a form of Petri net used in workflow management).

4. Analysis and Verification of Hybrid Systems

Hybrid systems (that is, dynamical systems with both continuous and discrete components) are commonly modeled by hybrid automata [ACHH93, Fre04, Hen96]. These, often highly complex, systems are usually nonlinear (making them computationally intractable as they are). However, linear approximations, which allow the use of polyhedral computations for the model checking operations, have been used successfully for the verification of useful safety properties [DHR05, FHK04, Fre04, Fre05, SCR06, SSM06].

In this section, we will illustrate, by means of examples, how polyhedral computations can be used for verifying simple properties of hybrid automata. The examples are all instances of *linear hybrid systems*, a particular class of hybrid systems that can be modeled using polyhedra where the continuous behavior is specified by linear constraints over the time-derivatives of the variables.

Definition 4.1. (Linear hybrid automaton.) A *linear hybrid automaton* (of dimension n) is a tuple

$$(\mathrm{Loc}, \mathrm{Init}, \mathrm{Act}, \mathrm{Inv}, \mathrm{Lab}, \mathrm{Trans})$$

where the first component Loc is a finite set of *locations*. For each location $\ell \in \mathrm{Loc}$, functions $\mathrm{Init}\colon \mathrm{Loc} \to \mathbb{P}_n$, $\mathrm{Act}\colon \mathrm{Loc} \to \mathbb{P}_n$ and $\mathrm{Inv}\colon \mathrm{Loc} \to \mathbb{P}_n$ define polyhedra. In particular: $\mathrm{Init}(\ell)$ specifies the set of possible initial values the n variables can take if the automaton starts at ℓ; $\mathrm{Act}(\ell)$ specifies the possible derivative values of the n variables, so that, if the automaton reaches ℓ with values given by the vector $\mathbf{v}$, then after staying there for a delay of $t \in \mathbb{R}$, the values will be given by a vector $\mathbf{v} + t\mathbf{w}$, where $\mathbf{w} \in \mathrm{Act}(\ell)$; $\mathrm{Inv}(\ell)$ specifies the values that an n-vector $\mathbf{v}$ may have at ℓ. The fifth and sixth components provide a set of *synchronization labels* Lab and a labeled set of affine transition relations $\mathrm{Trans} \subseteq \mathrm{Loc} \times \mathrm{Lab} \times \mathbb{P}_{2n} \times \mathrm{Loc}$, required to hold when moving from one location to the next.

Because the invariants of the system are given by means of convex polyhedra, this definition of a linear hybrid automaton differs from those in, for example [ACH$^+$95, Fre04, Hen96, HPR97], since there is no need to explicitly include a set of n variables as a component of the system.

The synchronization labels Lab are required for specifying large systems. Each part of the system is specified by a separate automaton, and then *parallel composition* is employed to combine the components into an automaton for the complete system. This ensures that communication between the automata occurs, via selected input/output variables, between transitions that have the same label. Example 4.4 provides a very simple illustration of parallel composition; formal definitions are available in [ACHH93, Hen96] and a larger application can be found in [MS00].

A linear hybrid automaton can be represented by a directed graph whose nodes are the locations and edges are the transitions from the source to the target locations. Each node ℓ is labeled by two sets of constraints defining the polyhedra $\mathrm{Inv}(\ell)$ and $\mathrm{Act}(\ell)$. To distinguish these constraints, if, for example x is a variable used for the constraints defining $\mathrm{Inv}(\ell)$, $\dot{x}$ will be used in the constraints defining $\mathrm{Act}(\ell)$.[6] In the examples, the initial polyhedron $\mathrm{Init}(\ell)$ is assumed to be empty unless there is an arrow to ℓ (with no source node) labeled by the constraint system defining $\mathrm{Init}(\ell)$. Each edge $\tau = \bigl(\ell, a, \mathcal{P}, \ell'\bigr) \in \mathrm{Trans}$, is labeled by the constraint system $\mathcal{C}$ defining $\mathcal{P}$ and, optionally, by a which is only included where it is used for the parallel composition of automata. Since $\mathcal{P} \in \mathbb{P}_{2n}$, we specify $\mathcal{C}$ by using two n-tuples of variables $\mathbf{x}$ and $\mathbf{x}'$, which are interpreted as usual to denote the variables in the source and target locations, respectively. We also adopt some helpful shorthand notation: $x{+}{+}$ and $x{-}{-}$ denotes $x' = x + 1$ and $x' = x - 1$, respectively; also, constraints of the form $x' = x$ are omitted. The following examples, taken (with some minor modifications) from [ACHH93, HPR97], illustrate the automata.

Example 4.2. A graphical view of a water-level monitor automaton is given in Figure 7. This models a system describing how the water level in a tank is controlled by a monitor that senses the water level w and turns a pump on and off. When the pump is off, w falls by 2 cms per second; when the pump is on, w rises by 1 cm per second. However, there is a delay of 2 seconds from the moment the monitor signals the pump to change from on to off or vice versa before the switch is actually operated. Initially the automaton is at ℓ_0 with $w = 1$ and it is required that $1 \leq w \leq 12$ at all times. Thus the monitor must signal the pump to turn on when $w = 5$ and signal it to turn off when $w = 10$.

The automaton illustrated in Figure 7 has 2 dimensions with variables w and x; where x denotes the time (in seconds) since the previous, most recent, signal from the monitor. There are four locations ℓ_i where $i = 0, 1, 2, 3$. At ℓ_0 and ℓ_1, the pump is on while at ℓ_2 and ℓ_3, the pump is off. At ℓ_1 and ℓ_3, the monitor has signaled a change to the pump switch but this is not yet been operated. Thus we

[6] The dot notation reflects the fact that these variables denote the derivatives of the state variables.

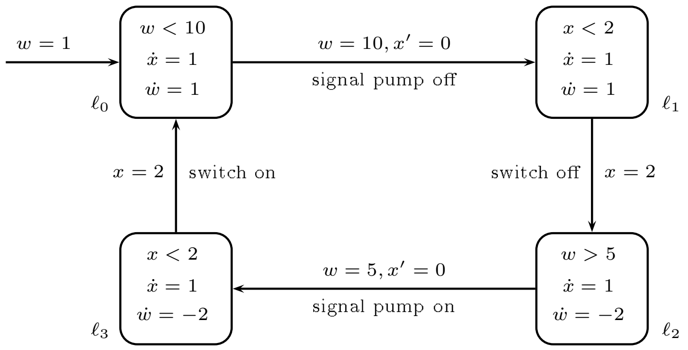


FIGURE 7. Water-level monitor

have:

$$\begin{aligned}
&\mathrm{Init}(\ell_1) = \mathrm{Init}(\ell_2) = \mathrm{Init}(\ell_3) = \emptyset, && \mathrm{Init}(\ell_0) = \mathrm{con}\bigl(\{w = 1\}\bigr),\\
&\mathrm{Inv}(\ell_0) = \mathrm{con}\bigl(\{w < 10\}\bigr), && \mathrm{Inv}(\ell_2) = \mathrm{con}\bigl(\{w > 5\}\bigr),\\
&\mathrm{Inv}(\ell_1) = \mathrm{Inv}(\ell_3) = \mathrm{con}\bigl(\{x < 2\}\bigr),\\
&\mathrm{Act}(\ell_0) = \mathrm{Act}(\ell_1) = \mathrm{con}\bigl(\{\dot{x} = \dot{w} = 1\}\bigr),\\
&\mathrm{Act}(\ell_2) = \mathrm{Act}(\ell_3) = \mathrm{con}\bigl(\{\dot{x} = 1, \dot{w} = -2\}\bigr).
\end{aligned}$$

There are four transitions $\tau_{ij} = (\ell_i, a_i, \mathcal{P}_i, \ell_j) \in \mathrm{Trans}$, where $i \in \{0, 1, 2, 3\}$ and $j = i + 1 \pmod 4$; the affine relations are

$$\begin{aligned}
\mathcal{P}_0 &= \mathrm{con}\bigl(\{w = 10, x' = 0, w' = w\}\bigr),\\
\mathcal{P}_1 &= \mathrm{con}\bigl(\{x = 2, x' = x, w' = w\}\bigr),\\
\mathcal{P}_2 &= \mathrm{con}\bigl(\{w = 5, x' = 0, w' = w\}\bigr),\\
\mathcal{P}_3 &= \mathcal{P}_1.
\end{aligned}$$

Example 4.3. A graphical representation of an automaton for a simplified version of the Fischer protocol is given in Figure 8. This models mutual exclusion for a system with two processors P_1 and P_2 with skewed clocks x_1 and x_2, respectively. Each processor has a critical section and, at any one moment in time, at most one may be in its critical section. This mutual exclusion is ensured by a version of the Fischer protocol which requires that P_1 and P_2 share a variable k; a process P_i ($i = 1$, 2) is only able to enter its critical section if $k = i$ and P_i may only write to k if $k = 0$. However, it takes at most a time units, as measured by P_i's clock for P_i to set the value of k to i and it could be that the other process P_j may also have started writing j to k. To avoid any resulting conflict, the protocol requires that P_i must wait for a further b time units, also measured by P_i's clock, before checking that $k = i$ still holds. The time b is called the *delay time*. The protocol ensures mutual exclusion only for certain values of a and b which depend on the relative rates of x_1 and x_2. Here it is assumed that the rate of x_2 is between 0.9 and 1.1 times that of x_1 and that, for $i = 1$, 2, the clock x_i is reset to zero at the start of both the write process and the delay time for P_i.

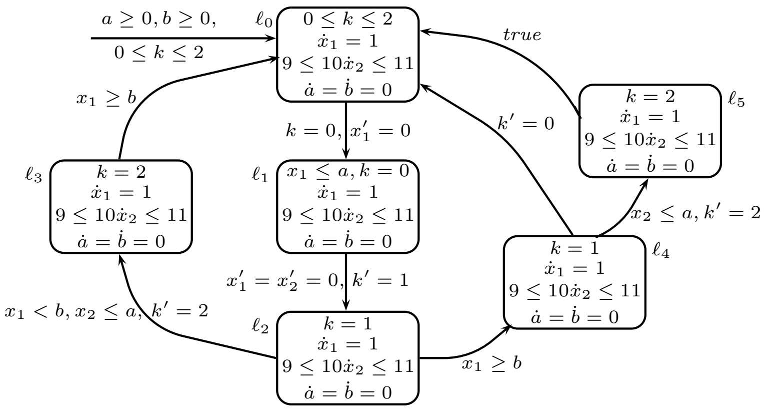


FIGURE 8. Fischer protocol (simplified)

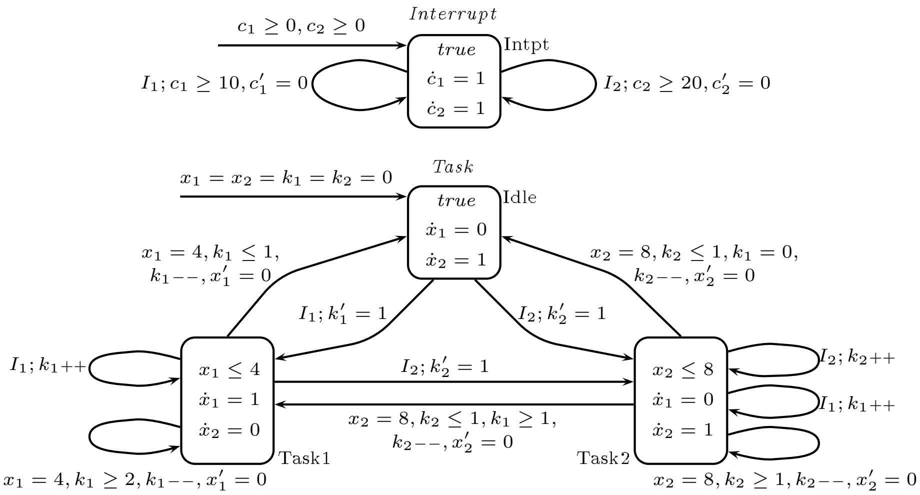


FIGURE 9. Scheduler

The automaton illustrated in Figure 8 has 5 dimensions with variables a, b, x_1, x_2, k. Note that here, a and b are constant for all runs of the automaton and this is indicated in the graph by the inclusion of the derivative constraints $\dot{a} = \dot{b} = 0$ at every location. There are six locations: ℓ_0 where P_1 is idle; at ℓ_1 where $k = 0$ and P_1 is in the process of writing to k; at ℓ_2 where $k = 1$ and P_1 waits for the delay time of b time units; at ℓ_3 where $k = 2$ since P_2 managed to complete writing to k before the delay time of b had expired; at ℓ_4 where the process P_1 is in the critical section; at ℓ_5 where P_2 has set $k = 2$ and the mutual exclusion guarantee is violated. All the functions and transitions for these locations are as given in Figure 8.

Example 4.4. A representation of an automaton for a simple task scheduler is given in Figure 9. This models a scheduler with two classes of tasks A_1 and A_2, activated by interrupts I_1 and I_2. Interrupt I_1 (resp., I_2) occurs at most once every

10 (resp., 20) seconds and activates a task in class A_1 (resp., A_2), which takes 4 (resp., 8) seconds to complete. Tasks in class A_2 have priority and preempt tasks in A_1. It is required that tasks in class A_2 never wait.

The automaton given in Figure 9 is the parallel composition of two component automata: *Interrupt*, which models the assumptions about the interrupt frequencies; and *Task*, which models the execution of the tasks. The *Interrupt* automaton, which has a single location 'Intpt', has 2 dimensions with variables c_1 and c_2; where the variable c_i $(i = 1, 2)$ measures the time elapsed since interrupt I_i occurred. The *Task* automaton has three locations: one labeled 'Idle' when no tasks are running and the other two labeled 'Task1' and 'Task2' for when task 1 (resp., task 2) is active. This automaton has 4 dimensions with variables x_1, x_2, k_1 and k_2. Letting $i = 1$, 2, the variable x_i measures the execution time of a task in class A_i, and k_i counts the number of pending tasks in class A_i. All the functions and transitions for both automata are as given in Figure 9.

The combined *Scheduler* automaton has 6 dimensions with variables x_1, x_2, k_1, k_2, c_1 and c_2. Its set of locations is formed by taking the Cartesian product of the sets of the component automata's locations. As the *Interrupt* component automaton has just one location, the locations for the product automaton are isomorphic to the locations for the *Task* automaton so that, for this simple example, these also denote the product locations. For each location ℓ in a product automaton, the initial $\mathrm{Init}(\ell)$, derivative $\mathrm{Act}(\ell)$ and invariant $\mathrm{Inv}(\ell)$ polyhedra are the concatenation of the corresponding component polyhedra for the *Task* and *Interrupt* automata (informally, a concatenation of polyhedra $\mathcal{P} \in \mathbb{P}_m$ and $\mathcal{Q} \in \mathbb{P}_n$ may be obtained by first embedding $\mathcal{P}$ into a vector space of dimension $n + m$ and then add a suitably renamed-apart version of the constraints defining $\mathcal{Q}$).

For each transition $(\ell, a, \mathcal{P}, \ell')$ in the *Task* automaton where $a \notin \{I_1, I_2\}$ (i.e., in the graphs, the label a is omitted), there is a transition $(\ell, a, \mathcal{Q}, \ell')$ in the product automaton where $\mathcal{Q} \in \mathbb{P}_6$ is obtained by embedding $\mathcal{P}$ into a vector space of dimension 6. Letting $i = 1$, 2, for transitions $(\ell, I_i, \mathcal{P}, \ell')$ and $(\mathrm{Intpt}, I_i, \mathcal{P}', \mathrm{Intpt})$ in the *Task* and *Interrupt* automata, respectively, there is a transition $(\ell, I_i, \mathcal{Q}, \ell')$ in the product automaton where $\mathcal{Q} \in \mathbb{P}_6$ is obtained by concatenating $\mathcal{P}$ and $\mathcal{P}'$ (and then reordering the dimensions so that variables for ℓ precede the variables for ℓ').

Given a linear hybrid automaton, the aim of an analyzer is to check, or even find sufficient conditions that ensure, that a valid *run* of the system cannot *reach* a location and vector of values that violates some requirement of the system. For instance, in Example 4.2, we need to show that the water level always lies between 1 cm and 12 cm; in Example 4.3, we need to find conditions on a and b so that at most one processor can be in its critical section at any one time; while in Example 4.4, we need to show that no class in A_2 will ever have to wait. To show how we can use polyhedral computations to prove such properties, we first need to define more formally such a run and how the reachable sets may be computed.

Letting $\mathcal{H} = (\mathrm{Loc}, \mathrm{Init}, \mathrm{Act}, \mathrm{Inv}, \mathrm{Lab}, \mathrm{Trans})$ be a linear hybrid automaton in n dimensions, a *state* s of $\mathcal{H}$ consists of a pair $(\ell, \mathbf{v})$, where $\ell \in \mathrm{Loc}$ and $\mathbf{v} \in \mathbb{R}^n$. Given states $s = (\ell, \mathbf{v})$ and $s' = (\ell', \mathbf{v}')$, a time delay $t \in \mathbb{R}_+$ and a vector $\mathbf{w} \in \mathrm{Act}(\ell)$,

$$s \rightarrow^t_{\mathbf{w}} s'$$

is a *step* of $\mathcal{H}$ provided that, for all $t' \in [0, t)$, $\mathbf{v} + t'\mathbf{w} \in \mathrm{Inv}(\ell)$ and, for some $(\ell, a, \mathcal{P}, \ell') \in \mathrm{Trans}$, $(\mathbf{v} + t\mathbf{w}) :: \mathbf{v}' \in \mathcal{P}$. A *run* of $\mathcal{H}$ is a sequence (finite or infinite) of steps

$$s_0 \to^{t_0}_{\mathbf{w}_0} s_1 \to^{t_1}_{\mathbf{w}_1} s_2 \cdots \tag{4.1}$$

where the initial state $s_0 = (\ell_0, \mathbf{v}_0)$ satisfies the condition $\mathbf{v}_0 \in \mathrm{Init}(\ell_0)$. An infinite run diverges if the sum $\sum_{i \geq 0} t_i$ diverges. For each divergent run given by (4.1) where, for $i \geq 0$, $s_i = (\ell_i, \mathbf{v}_i)$, we associate a (state) *behavior* β which is a total function from time to states: that is, for each $t \in \mathbb{R}_+$, $\beta(t) \stackrel{\text{def}}{=} (\ell_i, \mathbf{v})$, where

$$i = \min\left\{ k \in \mathbb{N} \;\middle|\; \sum_{j=0}^{k} t_j > t \right\} \qquad \text{and} \qquad \mathbf{v} = \mathbf{v}_i + \mathbf{w}_i\Bigl(t - \sum_{j<i} t_j\Bigr).$$

A state s is *reachable* if there exists a divergent run with behavior β and time $t \in \mathbb{R}_+$ such that $\beta(t) = s$. The set of all *reachable values* R_ℓ for a location ℓ is defined as:

$$R_\ell \stackrel{\text{def}}{=} \bigl\{\, \mathbf{v} \in \mathbb{R}^n \bigm| \exists t \in \mathbb{R}_+ \,.\, \beta(t) = (\ell, \mathbf{v}) \,\bigr\}.$$

The set of reachable values R_ℓ at a location ℓ can be characterized by a system of fixpoint equations that are defined in terms of sets of reachable values $R_{\ell'}$ at locations ℓ' where $\bigl(\ell', a, \mathcal{P}, \ell\bigr) \in \mathrm{Trans}$. These equations use the following operations on sets of vectors in $\mathbb{R}^n$. Let $\mathcal{P} \in \mathbb{P}_{2n}$ and $S \in \mathbb{R}^n$. Then

$$\psi_{\mathcal{P}}(S) \stackrel{\text{def}}{=} \bigl\{\, \mathbf{v}' \in \mathbb{R}^n \bigm| \mathbf{v} \in S, \mathbf{v} :: \mathbf{v}' \in \mathcal{P} \,\bigr\}.$$

Note that, if $S \in \mathbb{P}_n$, then $\psi_{\mathcal{P}}(S) \in \mathbb{P}_n$. Let $\mathcal{Q} \in \mathbb{P}_n$ and $S \in \mathbb{R}^n$. Then

$$S \nearrow \mathcal{Q} = \{\, \mathbf{v} + t\mathbf{w} \in \mathbb{R}^n \mid \mathbf{v} \in S, \mathbf{w} \in \mathcal{Q}, t \in \mathbb{R}_+ \,\}.$$

The '$\nearrow$' operator is called the *time elapse* operator. We can now provide the fixpoint equation for R_ℓ:

$$R_\ell = \biggl(\Bigl(\mathrm{Init}(\ell) \cup \bigcup_{(\ell', a, \mathcal{P}, \ell) \in \mathrm{Trans}} \psi_{\mathcal{P}}(R_{\ell'}) \cap \mathrm{Inv}(\ell)\Bigr) \nearrow \mathrm{Act}(\ell)\biggr) \cap \mathrm{Inv}(\ell). \tag{4.2}$$

Informally, the fixpoint equation for R_ℓ says that the reachable values at the location ℓ are obtained by letting the time elapse either from an initial value for ℓ or from a value obtained from an incoming transition. However, the fixpoint Equation (4.2) cannot handle strict constraints correctly and needs modifying; this is illustrated in the following example.

Example 4.5. Consider again Example 4.2. Then, just applying the Equation (4.2) (as proposed in [HPR94, HPR97]), the sets of reachable values at locations ℓ_1, ℓ_2, ℓ_3 are empty. The reason for this is that, for example, at location ℓ_0, the strict constraint $w < 10$ must hold, while in the transition from ℓ_0 to ℓ_1, the transition condition $w = 10$ has to hold. On the other hand, it follows from the definition of a step, that since one of the derivative constraints at ℓ_0 is $\dot{w} = 1$; the water level w may continue to increase up to the topological closure of R_{ℓ_0} which is consistent with $w = 10$.

To resolve this problem, in Equation (4.2) defining the concrete computation, $R_{\ell'}$ needs to be replaced by

$$c(R_{\ell'}) \cap \bigl(R_{\ell'} \nearrow \mathrm{Act}(\ell')\bigr), \tag{4.3}$$

where $c(R'_\ell)$ denotes the topological closure of R'_ℓ.

Observe that, although the linear hybrid automata are specified by means of polyhedra, the reachable set R_ℓ for a linear hybrid automaton and location ℓ may not be in the form of a convex polyhedron. Thus, to verify that some states of an automaton are unreachable using the standard polyhedral computations, approximations, even with such a restricted system, are needed. In particular, in the fixpoint Equation (4.2) (or (4.3)), the set operations have to be replaced by the corresponding polyhedral operations. In fact all the operations in (4.2) except set union can be used as they are since they transform polyhedra to polyhedra. Just the set union operation has to be replaced by the poly-hull operation $\uplus$ described in Section 2. Thus the following fixpoint equation computes an approximation $R_\ell^\sharp$ to the reachability set R_ℓ.

$$R_\ell^\sharp = \biggl(\Bigl(\mathrm{Init}(\ell) \uplus \biguplus_{(\ell',a,\mathcal{P},\ell)\in\mathrm{Trans}} \psi_{\mathcal{P}}(R_{\ell'}^\sharp) \cap \mathrm{Inv}(\ell)\Bigr) \nearrow \mathrm{Act}(\ell)\biggr) \cap \mathrm{Inv}(\ell). \tag{4.4}$$

As for the concrete fixpoint equation, to correctly handle the strict constraints Equation (4.4) needs to be be modified by replacing $R_{\ell'}^\sharp$ with

$$c(R_{\ell'}^\sharp) \cap \bigl(R_{\ell'}^\sharp \nearrow \mathrm{Act}(\ell')\bigr).$$

If we let $\mathbf{R}^\sharp$ denote the tuple $\{\, R_\ell^\sharp \mid \ell \in \mathrm{Loc}\,\}$ we can write Equation (4.4) as

$$R_\ell^\sharp = F_\ell(\mathbf{R}^\sharp)$$

For all $\ell \in \mathrm{Loc}$, we write $\mathbf{R}_\ell^{\sharp(0)} = \emptyset$ and, for all $k \geq 1$, $\mathbf{R}_\ell^{\sharp(k+1)} = F_\ell(\mathbf{R}_\ell^{\sharp(k)})$. Then $\mathbf{R}^\sharp$ can be computed iteratively provided the sequence $\mathbf{R}^{\sharp(0)}, \mathbf{R}^{\sharp(1)}, \ldots$ does not diverge. To handle diverging sequences, we apply a widening (see Section 7.2). Note that we do not have to apply it at all locations. Let $\mathcal{W}$ be a set of locations that cut all cyclic paths in the graph of the hybrid automaton (that is, each loop of the directed graph contains at least one location in $\mathcal{W}$). Then the following set of fixpoint equations is guaranteed to converge:

$$R_\ell^\sharp = \begin{cases} R_\ell^\sharp \mathbin{\nabla} F_\ell(\mathbf{R}^\sharp), & \text{if } \ell \in \mathcal{W}; \\ F_\ell(\mathbf{R}^\sharp), & \text{if } \ell \in \mathrm{Loc} \setminus \mathcal{W}. \end{cases} \tag{4.5}$$

Example 4.6. Consider again Example 4.2. As there is a single loop passing through ℓ_0, it is sufficient to define the set of widening locations as $\mathcal{W} = \{\ell_0\}$.

With the modified form of Equation (4.4) and the standard polyhedron widening, the computation requires three iterations resulting in polyhedra defined by constraint systems $\mathcal{C}_i$ for $0 \leq i \leq 3$ where:

$$\begin{aligned} \mathcal{C}_0 &= \{1 \leq w < 10\}, & \mathcal{C}_1 &= \{w - x = 10,\, 10 \leq w < 12\}, \\ \mathcal{C}_2 &= \{w + 2x = 16,\, 5 < w \leq 12\}, & \mathcal{C}_3 &= \{w + 2x = 5,\, 1 < w \leq 5\}. \end{aligned}$$

Example 4.7. Consider again Example 4.3. The analysis terminates without widening in just two iterations with the resulting polyhedron at ℓ_5 defined by the constraint system:

$$\begin{aligned} \mathcal{C} = \{k = 2,\, 10a \geq 9b,\, 0 \leq b \leq x_1,\, 9x_1 \leq 10x_2 \leq 11x_1,& \\ 11x_1 + 10a \geq 10x_2 + 11b\}.& \end{aligned}$$

It therefore follows that, to ensure that there can be no run with a state at location ℓ_5, it is sufficient that $10a < 9b$.

Example 4.8. Consider again Example 4.4. By applying the standard widening at location 'Task2' only, the analysis for the product automaton terminates in four iterations. After projecting away the variables c_1 and c_2, the reachable values are given by polyhedra defined by constraint systems $\mathcal{C}_{t0}$, $\mathcal{C}_{t1}$, and $\mathcal{C}_{t2}$ for locations 'Idle', 'Task1' and 'Task2', respectively, where:

$$\begin{aligned}
\mathcal{C}_{t0} &= \{x_1 = x_2 = k_1 = k_2 = 0\},\\
\mathcal{C}_{t1} &= \{0 \leq x_1 \leq 4,\, x_2 = 0, k_1 = 1,\, k_2 = 0\},\\
\mathcal{C}_{t2} &= \{x_2 \geq 0,\, x_2 \leq 8,\, 4k_1 \geq x_1,\, x_1 \geq 0,\, k_2 = 1\}.
\end{aligned}$$

So it can be concluded that, at each location of the automaton, $k_2 \leq 1$ and, hence, no task in class A_2 will ever have to wait. However, as noted in [HPR97], because of the convex hull approximation, with the polyhedral domain the analyzer fails to show that $k_1 \leq 2$. We therefore redid the analysis using a domain of powersets of polyhedra (see Section 6.2) and, after taking the poly-hull of the final sets and projecting away the variables c_1 and c_2, we obtained the polyhedra defined by constraint systems $\mathcal{C}'_{t0}$, $\mathcal{C}'_{t1}$ and $\mathcal{C}'_{t2}$ for locations 'Idle', 'Task1' and 'Task2', respectively, where:

$$\begin{aligned}
\mathcal{C}'_{t0} &= \{x_1 = x_2 = k_1 = k_2 = 0\},\\
\mathcal{C}'_{t1} &= \{0 \leq x_1 \leq 4,\, x_2 = 0,\, k_1 = 1,\, k_2 = 0\},\\
\mathcal{C}'_{t2} &= \{0 \leq x_1 \leq 4,\, 0 \leq x_2 \leq 8,\, 4k_1 \geq x_1 \geq 2k_1 - 2,\\
&\qquad\qquad x_1 + x_2 \geq 10k_1 - 10,\, k_1 \leq 2,\, k_2 = 1\}.
\end{aligned}$$

This verifies that $k_1 \leq 2$ and $k_0 \leq 1$ in every state of any run of the automata.

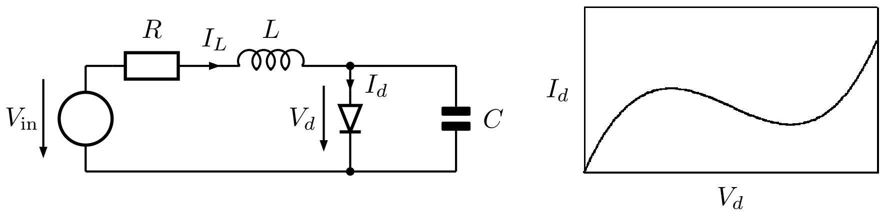
Hybrid systems with affine or nonlinear dynamics do not fit the above specification of a linear system so that the verification techniques described here are not directly applicable. Nonetheless, by partitioning the continuous state space and over-approximating the dynamics in each of the partitions, the same techniques used to verify linear hybrid automata can be used in these more general cases [DHR05, Fre05, HH95a, HHWT97, SSM06]. Such an approach has also been successfully applied in the verification of analog circuits, as discussed in the following section.

5. Analysis and Verification of Analog Systems

The idea of applying formal methods, that originated in the digital world, to analog systems was put forward in [HHB02]. This is an important step forward with respect to more traditional methods for the validation of analog circuit designs. A formal verification tool can, for example, ensure that a design satisfies certain properties for entire sets of initial states and continuous ranges of circuit parameters, something that cannot be done with simulation.

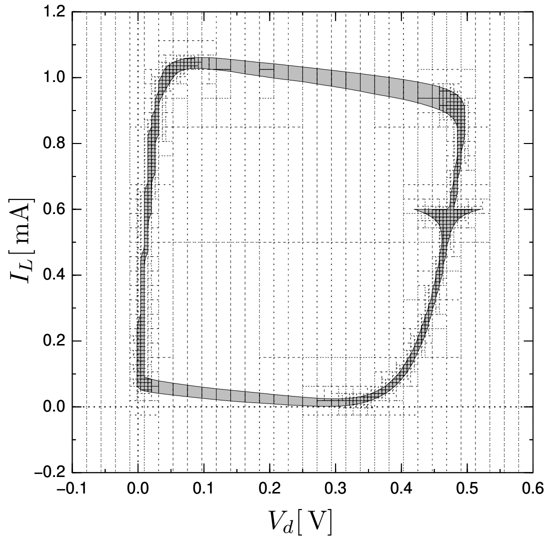
In [DDM04] and [GKR04], polyhedral approximations were successfully used in the verification of analog circuits. Here, we use a simple example, taken from [FKR06], on the verification of an oscillator circuit to illustrate the approach.[7] To verify properties of the (cyclic) behavior of such circuits, cyclic invariants have to be determined. To establish a cyclic invariant for a given set of initial states and ranges for the circuit parameters, one has to show that the circuit returns to a subset of

[7] For a more general view, we refer the interested reader to the cited literature and to [Mal06].



(a) Circuit schematic (b) Tunnel diode characteristic

FIGURE 10. Tunnel-diode oscillator circuit



(Picture courtesy of Goran Frehse.)

FIGURE 11. Reachable states of the tunnel-diode oscillator (dashed)

those initial states, which implies the system will keep traversing the same states indefinitely. From such an invariant, a number of properties of the oscillator can be established [FKRM06].

Consider the tunnel-diode oscillator schematized in Figure 10(a). The state of the system at a given instant of time is completely characterized by the values of the inductor current I_L and the diode voltage drop V_d. With these as the state variables, the system is described by the second-order state equations

$$\dot{V}_d = 1/C\bigl(-I_d(V_d) + I_L\bigr), \tag{5.1}$$

$$\dot{I}_L = 1/L(-V_d - RI_L + V_{\text{in}}). \tag{5.2}$$

In [FKR06] it is shown how a cyclic invariant can be obtained for this circuit using the PHAVer system. First, a piecewise affine envelope is constructed for the tunnel diode characteristic $I_d(V_d)$ depicted in Figure 10(b): for the particular example analyzed in [FKR06], sufficient precision is obtained by dividing the range $V_d \in [-0.1\,\mathrm{V}, 0.6\,\mathrm{V}]$ into 64 intervals, resulting in a piecewise affine model of (5.1). Forward reachability computation with PHAVer allows to obtain the set of states depicted in Figure 11. These are the states reachable from the set of initial states corresponding to $V_d \in [0.42\,\mathrm{V}, 0.52\,\mathrm{V}]$ and $I_L = 0.6\,\mathrm{mA}$ (the base of the downward-facing triangular shape in Figure 11). Taking into account that the loop shape constituted by the reachable states is traversed clockwise, it can be seen that the inductor current I_L returns to the initial value of $0.6\,\mathrm{mA}$ with a diode voltage drop that is well within the initial range $[0.42\,\mathrm{V}, 0.52\,\mathrm{V}]$. The set of reachable states so obtained is thus an invariant of the circuit.

In [FKR06] it is shown that, due to over-approximation, forward reachability can fail to determine invariants of more complex circuits. A new technique combining forward and backward reachability with iterative refinement of the partitions is thus proposed and shown to be more powerful and efficient.

6. Families of Polyhedral Approximations for Analysis and Verification

For several applications of static analysis and verification, an approximation based on the domain of convex polyhedra can be regarded as the most appropriate choice. In this section we discuss alternative options (simplifications, generalizations, and combinations with other numerical domains) that might be considered when trying either to reduce the cost of the analysis, or to increase the precision of the computed results.

6.1. Simplifications of Polyhedra. There are contexts where approximations based on the domain of convex polyhedra, no matter which implementation is adopted, incur an unacceptable computational cost. In such cases, the static analysis may resort to further simplifications so as to obtain useful results within reasonable time and space bounds.

A first, almost traditional approach is based on the identification of suitable syntactic subclasses of polyhedra. The abstract domain of *bounding boxes* (or intervals [CC76]) is based on polyhedra that can be represented as finite conjunctions of constraints of the form $\pm x_i \leq d$ or $\pm x_i < d$, leading to the specification of operations whose worst-case complexity is linear in the number of space dimensions. As a more precise alternative, the class of *potential constraints* [AK85, Bag97, Bel57, Dav87, Dil89, LLPY97], also known as *bounded differences*, allows for constraints of the form $x_i - x_j \leq d$ or $\pm x_i \leq d$; the generalization proposed in [BK89], also admits constraints of the form $x_i + x_j \leq d$, leading to the abstract domain of *octagons* [Min01]. In these last two cases, the operators are characterized by a worst-case time complexity which is cubic in the number of space dimensions. For all of the approximations mentioned above, improved efficiency also follows from the fact that the corresponding computations are simple enough to allow for the adoption of floating-point data types: in contrast, the specification of safe and efficient floating-point operations for general polyhedra is an open problem, so that polyhedra libraries have to be based on unbounded precision data types.

Several alternative (syntactic and/or semantic) simplification schemes have been put forward in the recent literature. The *Two Variables per Linear Inequality* abstract domain is proposed in [SKH02], where constraints take the syntactic form $ax_i + bx_j \leq d$. In [SSM05], an arbitrary family of polyhedra is chosen before starting the analysis by fixing the slopes of a finite number of linear inequalities, which are called the *template constraints*; linear programming techniques are then used to compute precise approximations in the considered class of shapes. In contrast, in [SCSM06], general polyhedra are allowed, but the corresponding operations (in particular, the poly-hull and the image of affine relations) are approximated by less precise variants so as to ensure a polynomial worst-case complexity in the size of the inputs. An even more flexible approach is proposed in [Fre05], where arbitrary polyhedra are approximated, when they become too complex, by limiting the number of constraints in their description and/or the magnitude of the coefficients occurring in the constraints. These more dynamic approximation schemes are promising, in particular for those applications where nothing is known in advance about the syntactic form of the constraints that will be computed during the analysis.

An important observation to be made is that there is no actual need to prefer *a priori* (and therefore commit to) a specific abstract domain: the analysis tool may be based on several abstractions, safely switching from more precise, possibly costly domains to more efficient, possibly imprecise ones, and vice versa, depending on the context. When replacing a generic polyhedron by a simpler one, the problem of the identification of a good over-approximation has to be solved. Depending on the context, the approaches may vary significantly. At one extreme, when efficiency is really critical, the adoption of syntactic techniques should be pursued: for an interesting example, we refer the reader to one of the simplification heuristics used in [Fre05], where the efficient selection of a small number of linear inequalities out of a constraint system is driven by a simple, yet effective reasoning on the measure of the angles formed by the corresponding half-spaces. At the other extreme, linear programming (LP) optimization techniques may be used so as to obtain the best match in the considered class of geometric shapes. For instance, the precise approximation of a polyhedron by a bounding box (resp., a bounded difference or octagon) can be implemented by a linear (resp., quadratic) number of optimizations of a class of LP problems, where the objective function varies while the feasible region is invariant and defined by the constraints of the polyhedron. Note that, if correctness has to be preserved, it is essential that no rounding error is made on the wrong side, so that classical floating-point implementations of LP solvers have to be considered unsafe, unless the computed results can be certified by some other tool. Alternatively, it is possible to consider LP implementations based on unbounded precision data types.

When the number of space dimensions to be modeled is beyond a given threshold, the whole analysis space can be split into a finite number of smaller, more manageable components, thereby realizing a further simplification scheme that can be combined with those described above. The splitting strategy varies considerably. In [HMPV03, HMG06], Cartesian factoring techniques are used so as to dynamically partition the space dimensions of a polyhedron into independent subsets; the orthogonal factors are then approximated by lower dimensional polyhedra with no precision penalty. In an alternative approach described in [BCC$^+$03], many (possibly overlapping) small subsets of space dimensions, called *variables packs*, are identified before the start of the analysis by means of syntactic conditions; the relations holding between the variables in each pack are then approximated by using an octagonal abstraction. A variation of this is described in [VB04], where non-overlapping variable packs are dynamically computed (and possibly merged) during the analysis, whereas the relations between the variables in a pack are approximated by means of potential constraints. In [VB04] it is also observed that, since the average size of variables packs is small (5 variables), more precise approximations based on general polyhedra should be feasible.

6.2. Generalizations of Polyhedra. There are applications where the restriction to the domain of convex polyhedra is intrinsically inadequate. This may happen, not only when the verification property of interest is itself non-convex, but also when the adopted computation strategy requires that a convex property is proved by passing through a non-convex intermediate approximation. This was the case in Example 4.8 of Section 4, where the upper bound ($k_1 \leq 2$) on the number of waiting processes for class A_1 was obtained by switching from the domain of convex polyhedra to the domain of finite sets of polyhedra.

The finite powerset domain construction [Bag98] is a special case of *disjunctive completion* [CC79], a systematic technique to derive an enhanced abstract domain starting from an existing one. A finite powerset domain implements disjunctions by maintaining an explicit (hence finite) and *non-redundant* collection of elements of the base-level domain: non-redundancy means that a collection is made of maximal elements with respect to the approximation ordering, so that no element subsumes another element in the collection.

For a better understanding of the concepts, which are described in completely general terms in [BHZ06c], let us consider the application of the finite powerset construction to the domain of convex polyhedra. This instantiation (which is the one also adopted for the examples developed in [BHZ06c]) can be used to model nonlinear systems as described, e.g., in Section 5. Then, an element of the abstract domain is a finite set of maximal convex polyhedra, so that no polyhedron in the set is contained in another polyhedron in the set. The powerset domain is a lattice: the bottom and top elements are $\emptyset$ and $\{\mathbb{R}^n\}$, respectively; the meet is obtained by removing redundancies from the set of all possible binary intersections of an element in the first powerset with an element in the second powerset; while the binary join is the non-redundant subset of the union of the two arguments. Most of the other abstract operations needed for a static analysis using the finite powerset domain are easily obtained by "lifting" the corresponding operations defined on the base-level domain, and then reinforcing non-redundancy. For instance, the computation of the image of a finite powerset under an affine relation is obtained by computing the image of each polyhedron in the collection. However, the construction of a provably correct widening operator has only recently been addressed in [BHZ06c] (see Section 7.2). The generic specification of the abstract operators of the finite powerset domain in terms of abstract operations on the (arbitrary) base-level domain allows for the development of a single implementation which is shared by all the possible instances of the domain construction.

An alternative abstraction scheme has been proposed in [BRCZ05] for the case of finite conjunctions of polynomial inequalities. Intuitively, a polynomial constraint can be approximated by means of a linear constraint in a higher dimension vector space, so that the different terms of the polynomial (e.g., x_0, x_0x_1, x_0^2) are mapped to different and independent space dimensions; these linear constraints are then used to perform an almost classical linear relation analysis based on convex polyhedra. Due to the linearization step, most of the precision of the polynomial constraints is initially lost; however, some of the relations holding between the different terms of the original polynomial can be recovered by adding further constraints that are redundant when interpreted in the polynomial world, but do contribute to precision in the linearized space. In particular, in [BRCZ05] the polynomial constraints are mapped into finitely generated *polynomial cones* and a degree-bounded product closure operator is systematically applied so as to improve accuracy. As a trivial example, let the polynomial terms x_0, x_1 and x_0x_1 be mapped to the space dimensions y_0, y_1 and y_2, respectively. Then, the linearization of the polynomial constraints $x_0 \geq 0$ and $x_1 \geq 0$ will produce a polyhedron that, while satisfying $y_0 \geq 0$ and $y_1 \geq 0$, leaves variable y_2 totally unconstrained. By applying the product closure operator we also obtain the linear constraint $y_2 \geq 0$, thereby recovering the non-negativity of term x_0x_1.

6.3. Combinations with other Numerical Abstractions. We observe that there are two basic kinds of numerical abstractions for approximating the values of the program variables: outer *limits* (or bounds within which the values must lie) and the pattern of *distribution* of these values. The first can be approximated by (constructions based on) convex polyhedra, while the second can be approximated by sets of congruences defining lattices of points we call *grids* [BDH+07, Gra91, Gra97]. Thus before considering how these and similar domains may be combined, we first give a brief overview of the domain of grids.

Any vector that satisfies $\langle \mathbf{a}, \mathbf{v} \rangle = b + \mu f$, for some $\mu \in \mathbb{Z}$, is said to *satisfy* the congruence relation $\langle \mathbf{a}, \mathbf{v} \rangle \equiv_f b$. A *congruence system* $\mathcal{C}\mathrm{g}$ is a finite set of congruence relations in $\mathbb{R}^n$. A *grid* is the set of all vectors in $\mathbb{R}^n$ that satisfy the congruences in $\mathcal{C}\mathrm{g}$. The domain of grids $\mathbb{G}_n$ is the set of all grids in $\mathbb{R}^n$ ordered by the set inclusion relation, so that the empty set and $\mathbb{R}^n$ are the bottom and top elements of $\mathbb{G}_n$ respectively and the intersection of two grids is itself a grid. Thus, as for the domain of polyhedra, the domain of grids forms a lattice $(\mathbb{G}_n, \subseteq, \emptyset, \mathbb{R}^n, \uplus, \cap)$ where $\uplus$ denotes the join operation returning the least grid greater than or equal to the two arguments. For more details concerning all aspects of the domain of grids, see [BDH+07].

The distribution information captured by grids has a number of applications in its own right, for instance: to ensure that external memory accesses obey the alignment restriction imposed by the host architecture; and to enable several transformations for efficient parallel execution as well as optimizations that enhance cache behavior. However, here we are primarily concerned with applications that can benefit from the combination of the domain of grids with that of convex polyhedra. For instance, knowing the frequency (and position) of the points in a grid, we can shrink the polyhedra so that the bounding hyperplanes pass through the grid values; if this leads to a polyhedron with reduced dimension (such as a single point) or one that is empty, it can lead, not only to improved precision, but also a more efficient use of resources by the analyzer [Anc91, NR00, QRR96].

Generic constructions such as direct and reduced product can be used to provide a formal basis for the combination of the grid and polyhedral domains [CC79]. However, the exact choice of product construction used to build the grid-polyhedral domain needs further study and should probably depend on the application. The problem is that the direct product has the disadvantage in that there is no provision for communication between the component domains while the reduced product, which is the most precise refinement of the direct product, has exponential complexity. It is expected that, for grid-polyhedra, the most useful product construction will lie between these extremes. For instance, as equalities are common entities for both constraint and congruence systems, if an equality is found to hold in one component, it is safe to just add this to the constraint or congruence system describing the other component. In addition, any hyperplane that bounds the polyhedron could be moved inwards until it intersect with points of the grid with only linear cost on the number of dimensions. Of course, this reduction on its own is not optimal since the grid points in the intersection may not lie in the polyhedron itself. For optimality or, more generally, so as to gain additional precision, we need to experiment with various forms of the branch-and-bound and cutting-plane algorithms [KM06] already well-researched for integer linear programming. What is needed is a range of options for the product construction allowing the user to decide on the complexity/precision trade-off. Further work on this including an investigation of other proposals for generic products that lie between the direct and reduced product such as the local decreasing iteration method [Gra92] and the open product construction [CLV00] is needed.

7. Polyhedral Computations Peculiar to Analysis and Verification

As observed in the previous sections, the analysis of the run-time behavior of a system can be traced down to the computations of a basic set of operations on the chosen abstract domains. This means that each abstract domain should provide adequate computational support for such a set and, where appropriate, further operations that might be useful for tuning the cost/precision ratio. In this section, we discuss several key issues relevant to the design and implementation of an abstract domain of, or based on, convex polyhedra. Before going into further detail, it should be stressed that the particular context of application plays a significant and non-trivial role here. For instance, in many computational complexity studies, it is assumed that a small number of operations (often, just a single one) will have operands whose sizes can grow arbitrarily large; also, it is typically required that exact results have to be computed. Both these assumptions may be inappropriate in the context of static analysis: it is quite often the case that a large number of operations will have only small or medium sized operands; moreover, whenever facing an efficiency issue, the exactness requirement can be dropped (provided soundness is maintained). As a consequence, the evaluation of alternative algorithmic strategies should be based on practical experimentation, rather than purely theoretical results.

7.1. The Double Description Method. Convex polyhedra are typically specified by a finite system of linear inequality constraints and there are known algorithms (e.g., based on Fourier-Motzkin elimination [LM92, Sch99]) for computing most of the operations already mentioned on such a description.

An alternative approach is based on the *double description* method due to Motzkin et al. [MRTT53]. This method was originally defined on the set of topologically closed convex polyhedra, a sub-lattice $(\mathbb{CP}_n, \subseteq, \emptyset, \mathbb{R}^n, \uplus, \cup)$ of the lattice of (not necessarily closed, or NNC) polyhedra $\mathbb{P}_n$. In the double description method, a closed polyhedron may be described by using a system of non-strict linear inequalities or by using a *generator* system that records its key geometric features. The following is the main theoretical result, which is a simple consequence of well-known theorems by Minkowski and Weyl [SW70].

Theorem 7.1. *The set $\mathcal{P} \subseteq \mathbb{R}^n$ is a topologically closed convex polyhedron if and only if there exist finite sets $R, P \subseteq \mathbb{R}^n$ of cardinality r and p, respectively, such that $\mathbf{0} \notin R$ and $\mathcal{P}$ can be generated from (R, P) as follows:*

$$\mathcal{P} = \left\{ R\rho + P\pi \in \mathbb{R}^n \;\middle|\; \rho \in \mathbb{R}^r_+, \pi \in \mathbb{R}^p_+, \textstyle\sum_{i=1}^p \pi_i = 1 \right\}.$$

Intuitively, a point of a polyhedron $\mathcal{P}$ is obtained by adding a convex combination of the vectors in P (the generating points) to a conic combination of the vectors in R (the generating *rays*).

It turns out that constraint and generator descriptions are duals: each representation can be computed starting from the other one. Clever implementations of this conversion procedure, improving on the Chernikova's algorithms [Che64, Che65, Che68], are the starting point for the development of software libraries that, while being characterized by a worst case computational cost which is exponential in the size of the input, turn out to be practically useful. A common characteristic of these implementations is the exploitation of *incrementality*, whereby most of the computational work done for an operation is reused to efficiently compute small variations of the corresponding result. Further computational enhancements are obtained by the adoption of suitable heuristics, ranging from the efficient handling of adjacency information [Le 92], to a careful choice of ordering strategies for the computation of intermediate results [Avi00, AB95, FP96]; the overall construction typically relies on a tight integration of the basic algorithms with a carefully chosen set of data structures [BHZ06b].

An important motivation for the adoption of an implementation based on the double description method is that the ability to switch from a constraint description to a generator description, or vice versa, can be usefully exploited to provide simple implementations for the basic operations on polyhedra. For instance, set intersection is easily implemented by taking the union of the constraint systems representing the two arguments, whereas the poly-hull is implemented by joining the generator systems representing the two arguments; and the test for emptiness can be implemented by checking whether the generator system contains no points at all. Moreover, a test for subset inclusion $\mathcal{P} \subseteq \mathcal{Q}$ can be implemented by checking if each point and each ray in a generator system describing $\mathcal{P}$ satisfies all linear inequalities in a constraint system describing $\mathcal{Q}$. As a further example, the time elapse operation specified in Section 4 can be implemented using the generator systems for the argument polyhedra. That is, a generator system for the polyhedron $\mathcal{P} \nearrow \mathcal{Q}$ can be obtained by adopting the same set of generating points as $\mathcal{P}$ and by defining its set of rays as the union of the set of generating rays for $\mathcal{P}$ with the set of all the generators (both points and rays) for $\mathcal{Q}$.

As seen in Section 3, in the context of the analysis of imperative languages one of the most frequent statements is variable assignment, where the expression assigned is safely approximated by an affine relation $\psi \subseteq \mathbb{R}^n \times \mathbb{R}^n$. The (direct or inverse) image of an affine relation can be naively computed by embedding the input polyhedron $\mathcal{P} \subseteq \mathbb{R}^n$ into the space $\mathbb{R}^{2n}$, intersecting it with the constraints defining ψ and finally projecting the result back on $\mathbb{R}^n$. However, due to the moves to/from a higher dimensional space, this approach suffers from significant overheads. Quite often, the expression assigned is a simple affine function of the variables' values and can thus be exactly modeled by computing the image of a single-update affine function. With the double description method, the images of affine functions are much more efficiently computed by applying them directly to the generators of the argument polyhedron. A dual approach, using the constraint description of the polyhedron, allows for the computation of the preimages of affine functions, which can be of interest for a backward semantic construction, where the initial values of program variables are approximated starting from their final values. Similar efficiency arguments motivate the study of specific implementations for single-update bounded affine relations and other special subclasses of affine relations.

7.2. Widening and Narrowing. The first widening operator for the domain of convex polyhedra, proposed in [CH78] and refined in [Hal79], can be informally described as follows: suppose that in the post-fixpoint iteration sequence we compute as successive iterates the polyhedra $\mathcal{P}_i$ and $\mathcal{P}_{i+1}$; then, the widening keeps all and only the constraints defining $\mathcal{P}_i$ that are also satisfied by $\mathcal{P}_{i+1}$. This simple idea, which is basically borrowed from the widening operator defined on the domain of intervals [CC76], is quite effective in ensuring the termination of the analysis (the number of constraints decreases at each iteration); by avoiding the application of the widening in the first few iterations of the analysis [Cou81] and/or by applying the "widening up-to" technique of [Hal93], it also provides, in the main, an adequate level of precision.

Some application fields, however, are particularly sensitive to the precision of the deduced numerical information, to the point that some authors propose to give up the termination guarantee and use so-called *extrapolation* operators: examples include the operators defined in [HPWT01] and [HH95b], as well as the proposals in [BGP99] and [DP99] for sets of polyhedra and the heuristics sketched in [BJT99].

In [BHRZ05] this precision problem is reconsidered in a more general context and a framework is proposed that is able to improve upon the precision of a given widening while keeping the termination guarantee. The approach, which builds on theoretical results put forward in work on termination analysis, combines an existing widening operator, whose termination guarantee should be *formally certifiable*, with an arbitrary number of precision improving heuristics. Its feasibility was demonstrated by instantiating the framework so as to produce a new widening on polyhedra improving upon the precision of [Hal79] in a significant percentage of benchmarks.

For the more challenging case of an abstract domain obtained by the finite powerset domain construction, several generic schemes of widenings have been proposed in [BHZ06c] that are able to "lift" a widening defined on the base-level domain without compromising its termination guarantee. The instantiation of such a generic approach led to the definition of the first non-trivial and provably correct widenings on a domain of finite sets of convex polyhedra. Being highly parametric, the widening schemes proposed in [BHZ06c] can be instantiated according to the needs of the specific application, as done in [GR06]. One of the heuristic approaches adopted in [BHZ06c] to control the precision/complexity trade-off of the widenings, originally proposed in [BGP99], attempts at reducing the cardinality of a polyhedral collection by merging two of its elements whenever their set union happens to be a convex polyhedron. The implementation of such a heuristics could significantly benefit from the results and algorithms presented in [BF05, BFT01].

It is also worth mentioning that, once a post-fixpoint approximation has been obtained by means of an upward iteration sequence with widening, its precision can be improved by means of a downward iteration, possibly using a *narrowing operator* [CC77, CC76, CC92a, CC92b]. To the best of our knowledge, no narrowing has ever been defined on the domain of convex polyhedra: applications simply stop the downward computation after a small number of iterations.

7.3. Not Necessarily Closed Convex Polyhedra. Most static analysis applications computing linear inequality relations between program variables consider the domain $\mathbb{CP}_n$ of topologically closed polyhedra. One of the underlying motivations is that sometimes (e.g., when working with integer valued variables only) strict inequalities can be filtered away by suitable syntactic manipulations; even when this is not the case, the topological closure approximation may be interpreted as a quick and practical workaround to the fact that some software libraries do not fully support computations on NNC polyhedra. However, there are applications [ACHH93, CS01, HPR94, HPR97] where the ability of encoding and propagating strict inequalities might be crucial for the usefulness of the final results.

The first proposal for a systematic implementation of strict inequalities in a software library based on the double description method was put forward in [HPR94]: a syntactic translation embeds an n-dimensional NNC polyhedron $\mathcal{P} \in \mathbb{P}_n$ into an $(n+1)$-dimensional closed polyhedron $\mathcal{R} \in \mathbb{CP}_{n+1}$, by adding a single *slack variable* ϵ, satisfying the additional side constraints $0 \leq \epsilon \leq 1$. Namely, any strict inequality constraint $\langle \mathbf{a}, \mathbf{x} \rangle > b$ is translated into the non-strict inequality constraint $\langle \mathbf{a}, \mathbf{x} \rangle - \epsilon \geq b$. The computation is thus performed on the closed representation $\mathcal{R} \in \mathbb{CP}_{n+1}$, with only minor adaptations to the basic algorithms so as to also take into account the *implicit* strict constraint $\epsilon > 0$.

While this idea is quite effective, the resulting software library no longer enjoys all of the properties of the underlying double description implementation: NNC polyhedra cannot be suitably described using generator systems, and the geometric intuitions are lost under the "implementation details." These problems motivated the studies in [BHZ03, BHZ05, BRZH02], where a proper generalization of the double description method to NNC polyhedra was proposed. The main improvement was the identification of the *closure point* as a new kind of generator for NNC polyhedra, leading to the following result generalizing Theorem 7.1.

Theorem 7.2. *The set $\mathcal{P} \subseteq \mathbb{R}^n$ is an NNC polyhedron if and only if there exist finite sets $R, P, C \subseteq \mathbb{R}^n$ of cardinality r, p and c, respectively, such that $\mathbf{0} \notin R$ and*

$$\mathcal{P} = \left\{ R\rho + P\pi + C\gamma \in \mathbb{R}^n \;\middle|\; \begin{array}{l} \rho \in \mathbb{R}_+^r, \pi \in \mathbb{R}_+^p, \pi \neq \mathbf{0}, \gamma \in \mathbb{R}_+^c, \\ \sum_{i=1}^p \pi_i + \sum_{i=1}^c \gamma_i = 1 \end{array} \right\}.$$

The new condition $\pi \neq \mathbf{0}$ ensures that at least one of the points of P plays an active role in any convex combination of the vectors of P and C. As a consequence, the vectors of C are closure points of $\mathcal{P}$, i.e., points that belong to the topological closure of $\mathcal{P}$, but may not belong to $\mathcal{P}$ itself.

Thanks to the introduction of (strict inequalities and) closure points, most of the pros of the double description method now also apply to the domain of NNC polyhedra: simpler, higher-level implementations of operations on NNC polyhedra can be specified, reasoned about and justified in terms of any one of the two dual descriptions; important implementation issues (such as the need to identify and remove all kinds of redundancies in the descriptions [BHZ05, BRZH02]) can be provided with proper solutions; different lower-level encodings (e.g., an alternative management of the slack variable [BHZ03, BHZ05]) can be investigated and experimented with, without affecting the user of the software library. It would be interesting, from both a theoretical and practical point of view, to provide a more direct encoding of NNC polyhedra, i.e., one that is not based on the use of slack variables; this requires the specification and the corresponding proof of correctness of a direct NNC conversion algorithm, potentially achieving a major efficiency improvement.

8. Conclusion

In the field of automatic analysis and verification of software and hardware systems, approximate reasoning on numerical quantities is crucial. As first recognized in 1978 [CH78], polyhedral computation algorithms can be used for the automatic inference of numerical assertions that correctly (though usually not completely) characterize the behavior of a system at some level of abstraction.

Until the end of the 1990's these techniques were not in widespread use, mainly due to the unavailability of robust and efficient implementations of convex polyhedra. As far as we know, the first published libraries of polyhedral algorithms suitable for analysis and verification purposes have been *Polylib*,[8] released in 1995, written by Wilde at IRISA [Wil93] and based on earlier work by Le Verge [Le 92], and the polyhedra library of *POLINE* (POLyhedra INtegrated Environment) written by Halbwachs and Proy at Verimag and also released in 1995. Both libraries used machine integers to represent the coefficients of linear equalities and inequalities, something that could easily result into (undetected) overflows. While Polylib provided only a fraction of the functionalities offered by POLINE's library (which offered, among other things, support for NNC polyhedra), it was available in source format. The POLINE's library, instead, was distributed only in binary form for the Sun-4 platform (freely, until about the year 1996; under rather restrictive conditions afterward). POLINE included also a system called POLKA (POLyhedra desK cAlculator) and an analyzer for linear hybrid automata. A variation of a subset of POLINE's library was incorporated into the *HyTech* tool [HHWT97].[9]

The work of Wilde and Le Verge, which was extended by Loechner [Loe99], led to the creation of *PolyLib*.[10] The *New Polka* library by Jeannet,[11] first released in 2000 and originally based on both IRISA's Polylib and POLINE's library, incorporates the idea —suggested by Fukuda and Prodon [FP96]— of lexicographically sorting the matrices representing constraints and generators. New Polka, which supports both closed and NNC polyhedra, together with Miné's *Octagon Abstract Domain Library* [Min01, Min05][12] and an interval library called *ITV*, is now included in the *APRON* library.[13] Finally, the *Parma Polyhedra Library* (PPL), initially inspired by New Polka and first released in 2001, is developed and maintained by the authors of this paper.[14] The PPL supports both closed and NNC polyhedra, bounding boxes, bounded difference and octagonal shapes, grids and combinations of the above including the finite powerset construction [BHZ06a].

The above libraries have all been designed specifically for applications of analysis and verification such as those described in this paper. However, two libraries that

[8] `http://www.ee.byu.edu/faculty/wilde/polyhedra.html`.
[9] `http://embedded.eecs.berkeley.edu/research/hytech/`.
[10] `http://icps.u-strasbg.fr/polylib/`.
[11] `http://pop-art.inrialpes.fr/people/bjeannet/newpolka/index.html`.
[12] `http://www.di.ens.fr/~mine/oct/`
[13] `http://apron.cri.ensmp.fr/library/`.
[14] `http://www.cs.unipr.it/ppl`.

were designed for solving vertex enumeration/convex hull problems have successfully been used in static analysis and computer-aided verification tools: Fukuda's *cddlib*,[15] an implementation of the double description method [MRTT53]; and *lrslib*,[16] the implementation by Avis of the reverse search algorithm [Avi00].

All the libraries mentioned in the last two paragraphs are distributed under free software licenses and support the use of unbounded numeric coefficients. This, together with the ever increasing available computing power and the growing interest in ensuring the correctness of critical systems, has caused, in the 2000's, the continuous emergence of new tools and applications of polyhedral computations in the area of formal methods. As a consequence, this is much more of a new beginning than an end to research in this area. As explained in Sections 6 and 7, several open issues remain. Most of them have to do with the need for effectively managing the complexity-precision trade-off: the encouraging results obtained with today's tools push us to apply them to more complex systems for a possibly more precise analysis and/or verification of more complex properties. Further progress in this area calls for a tight collaboration of experts in the fields of formal methods, computational geometry and combinatorial optimization. We hope the present paper constitutes a useful step in this direction.

Acknowledgments

We thank Goran Frehse for the discussion we had on the subject of polyhedra simplifications and for contributing the PostScript code we used to produce Figure 11. The first author would also like to thank the organizers and participants of the *Polyhedral Computation* workshop[17] for providing the environment and initial inspiration that brought us to write this paper.

References

[AB95] D. Avis and D. Bremner, *How good are convex hull algorithms?*, Proceedings of the Eleventh Annual Symposium on Computational Geometry (Vancouver, B.C., Canada), ACM Press, 1995, pp. 20–28.

[ACH+95] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X Nicollin, A. Olivero, J. Sifakis, and S. Yovine, *The algorithmic analysis of hybrid systems*, Theoretical Computer Science **138** (1995), 3–34.

[ACHH93] R. Alur, C. Courcoubetis, T. A. Henzinger, and P.-H. Ho, *Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems*, Hybrid Systems I, Lecture Notes in Computer Science, vol. 736, 1993, pp. 209–229.

[AH83] G. Alefeld and J. Herzberger, *Introduction to interval computation*, Academic Press, New York, 1983.

[AK85] J. F. Allen and H. A. Kautz, *A model of naive temporal reasoning*, Formal Theories of the Commonsense World (J. R. Hobbs and R. Moore, eds.), Ablex, Norwood, NJ, 1985, pp. 251–268.

[Anc91] C. Ancourt, *Génération automatique de codes de transfert pour multiprocesseurs à mémoires locales*, Ph.D. thesis, Université de Paris VI, Paris, France, March 1991.

[Avi00] D. Avis, *lrs: A revised implementation of the reverse search vertex enumeration algorithm*, Polytopes — Combinatorics and Computation (G. Kalai and G. M. Ziegler, eds.), Oberwolfach Seminars, vol. 29, Birkhäuser-Verlag, 2000, pp. 177–198.

---

[15] `http://www.ifor.math.ethz.ch/~fukuda/cdd_home/`.

[16] `http://cgm.cs.mcgill.ca/~avis/C/lrs.html`.

[17] Centre de recherches mathématiques, Université de Montréal, Montréal (Québec), Canada, October 17–20, 2006.

[Bag97] R. Bagnara, *Data-flow analysis for constraint logic-based languages*, Ph.D. thesis, Dipartimento di Informatica, Università di Pisa, Pisa, Italy, March 1997, Printed as Report TD-1/97.

[Bag98] ———, *A hierarchy of constraint systems for data-flow analysis of constraint logic-based languages*, Science of Computer Programming **30** (1998), no. 1–2, 119–155.

[BCC+03] B. Blanchet, P. Cousot, R. Cousot, J. Feret, L. Mauborgne, A. Miné, D. Monniaux, and X. Rival, *A static analyzer for large safety-critical software*, Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation (PLDI'03) (San Diego, California, USA), ACM Press, 2003, pp. 196–207.

[BDH+07] R. Bagnara, K. Dobson, P. M. Hill, M. Mundell, and E. Zaffanella, *Grids: A domain for analyzing the distribution of numerical values*, Logic-based Program Synthesis and Transformation, 16th International Symposium (Venice, Italy) (G. Puebla, ed.), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2007, To appear.

[Bel57] R. Bellman, *Dynamic programming*, Princeton University Press, 1957.

[BF05] I. Bárány and K. Fukuda, *A case when the union of polytopes is convex*, Linear Algebra and its Applications **397** (2005), 381–388.

[BFT01] A. Bemporad, K. Fukuda, and F. D. Torrisi, *Convexity recognition of the union of polyhedra*, Computational Geometry: Theory and Applications **18** (2001), no. 3, 141–154.

[BGP99] T. Bultan, R. Gerber, and W. Pugh, *Model-checking concurrent systems with unbounded integer variables: Symbolic representations, approximations, and experimental results*, ACM Transactions on Programming Languages and Systems **21** (1999), no. 4, 747–789.

[BHP+07] R. Bagnara, P. M. Hill, A. Pescetti, and E. Zaffanella, *On the design of generic static analyzers for modern imperative languages*, Quaderno, Dipartimento di Matematica, Università di Parma, Italy, 2007. Available at `http://www.cs.unipr.it/Publications/`.

[BHRZ05] R. Bagnara, P. M. Hill, E. Ricci, and E. Zaffanella, *Precise widening operators for convex polyhedra*, Science of Computer Programming **58** (2005), no. 1–2, 28–56.

[BHZ03] R. Bagnara, P. M. Hill, and E. Zaffanella, *A new encoding and implementation of not necessarily closed convex polyhedra*, Proceedings of the 3rd Workshop on Automated Verification of Critical Systems (Southampton, UK) (M. Leuschel, S. Gruner, and S. Lo Presti, eds.), 2003, Published as TR Number DSSE-TR-2003-2, University of Southampton, pp. 161–176.

[BHZ05] ———, *Not necessarily closed convex polyhedra and the double description method*, Formal Aspects of Computing **17** (2005), no. 2, 222–257.

[BHZ06a] ———, *The Parma Polyhedra Library: Toward a complete set of numerical abstractions for the analysis and verification of hardware and software systems*, Quaderno 457, Dipartimento di Matematica, Università di Parma, Italy, 2006. Available at `http://www.cs.unipr.it/Publications/`. Also published as `arXiv:cs.MS/0612085`, available from `http://arxiv.org/`.

[BHZ06b] ———, *The Parma Polyhedra Library user's manual*, Department of Mathematics, University of Parma, Parma, Italy, release 0.9 ed., March 2006. Available at `http://www.cs.unipr.it/ppl/`.

[BHZ06c] ———, *Widening operators for powerset domains*, Software Tools for Technology Transfer **8** (2006), no. 4/5, 449–466. (As the figures in the journal version of this paper have been improperly printed —rendering them useless— interested readers are recommended to download an electronic copy or contact one of the authors for a printed copy.)

[Bir67] G. Birkhoff, *Lattice theory*, third ed., Colloquium Publications, vol. XXV, American Mathematical Society, Providence, Rhode Island, USA, 1967.

[BJT99] F. Besson, T. P. Jensen, and J.-P. Talpin, *Polyhedral analysis for synchronous languages*, Static Analysis: Proceedings of the 6th International Symposium (Venice, Italy) (A. Cortesi and G. Filé, eds.), Lecture Notes in Computer Science, vol. 1694, Springer-Verlag, Berlin, 1999, pp. 51–68.

[BK89] V. Balasundaram and K. Kennedy, *A technique for summarizing data access and its use in parallelism enhancing transformations*, Proceedings of the ACM SIGPLAN'89 Conference on Programming Language Design and Implementation (PLDI) (Portland, Oregon, USA) (B. Knobe, ed.), ACM SIGPLAN Notices, vol. 24(7), ACM Press, 1989, pp. 41–53.

[BRCZ05] R. Bagnara, E. Rodríguez-Carbonell, and E. Zaffanella, *Generation of basic semi-algebraic invariants using convex polyhedra*, Static Analysis: Proceedings of the 12th International Symposium (London, UK) (C. Hankin and I. Siveroni, eds.), Lecture Notes in Computer Science, vol. 3672, Springer-Verlag, Berlin, 2005, pp. 19–34.

[BRZH02] R. Bagnara, E. Ricci, E. Zaffanella, and P. M. Hill, *Possibly not closed convex polyhedra and the Parma Polyhedra Library*, Static Analysis: Proceedings of the 9th International Symposium (Madrid, Spain) (M. V. Hermenegildo and G. Puebla, eds.), Lecture Notes in Computer Science, vol. 2477, Springer-Verlag, Berlin, 2002, pp. 213–229.

[CC76] P. Cousot and R. Cousot, *Static determination of dynamic properties of programs*, Proceedings of the Second International Symposium on Programming (Paris, France) (B. Robinet, ed.), Dunod, Paris, France, 1976, pp. 106–130.

[CC77] ———, *Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints*, Proceedings of the Fourth Annual ACM Symposium on Principles of Programming Languages (New York), ACM Press, 1977, pp. 238–252.

[CC79] ———, *Systematic design of program analysis frameworks*, Proceedings of the Sixth Annual ACM Symposium on Principles of Programming Languages (New York), ACM Press, 1979, pp. 269–282.

[CC92a] ———, *Abstract interpretation frameworks*, Journal of Logic and Computation **2** (1992), no. 4, 511–547.

[CC92b] ———, *Comparing the Galois connection and widening/narrowing approaches to abstract interpretation*, Proceedings of the 4th International Symposium on Programming Language Implementation and Logic Programming (Leuven, Belgium) (M. Bruynooghe and M. Wirsing, eds.), Lecture Notes in Computer Science, vol. 631, Springer-Verlag, Berlin, 1992, pp. 269–295.

[CC92c] ———, *Inductive definitions, semantics and abstract interpretation*, Proceedings of the Nineteenth Annual ACM Symposium on Principles of Programming Languages, ACM Press, 1992, pp. 83–94.

[CH78] P. Cousot and N. Halbwachs, *Automatic discovery of linear restraints among variables of a program*, Conference Record of the Fifth Annual ACM Symposium on Principles of Programming Languages (Tucson, Arizona), ACM Press, 1978, pp. 84–96.

[Che64] N. V. Chernikova, *Algorithm for finding a general formula for the non-negative solutions of system of linear equations*, U.S.S.R. Computational Mathematics and Mathematical Physics **4** (1964), no. 4, 151–158.

[Che65] ———, *Algorithm for finding a general formula for the non-negative solutions of system of linear inequalities*, U.S.S.R. Computational Mathematics and Mathematical Physics **5** (1965), no. 2, 228–233.

[Che68] ———, *Algorithm for discovering the set of all solutions of a linear programming problem*, U.S.S.R. Computational Mathematics and Mathematical Physics **8** (1968), no. 6, 282–293.

[CLV00] A. Cortesi, B. Le Charlier, and P. Van Hentenryck, *Combinations of abstract domains for logic programming: Open product and generic pattern construction*, Science of Computer Programming **38** (2000), no. 1–3, 27–71.

[Cou81] P. Cousot, *Semantic foundations of program analysis*, Program Flow Analysis: Theory and Applications (S. S. Muchnick and N. D. Jones, eds.), Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1981, pp. 303–342.

[Cou05] ———, *Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming*, Verification, Model Checking and Abstract Interpretation: Proceedings of the 6th International Conference (VMCAI 2005) (Paris, France) (R. Cousot, ed.), Lecture Notes in Computer Science, vol. 3385, Springer-Verlag, Berlin, 2005, pp. 1–24.

[CS01] M. A. Colón and H. B. Sipma, *Synthesis of linear ranking functions*, Tools and Algorithms for Construction and Analysis of Systems, 7th International Conference, TACAS 2001 (Genova, Italy) (T. Margaria and W. Yi, eds.), Lecture Notes in Computer Science, vol. 2031, Springer-Verlag, Berlin, 2001, pp. 67–81.

[Dav87] E. Davis, *Constraint propagation with interval labels*, Artificial Intelligence **32** (1987), no. 3, 281–331.

[DDM04] T. Dang, A. Donzé, and O. Maler, *Verification of analog and mixed-signal circuits using hybrid system techniques*, Proceedings of the 5th International Conference on Formal Methods in Computer-Aided Design (Austin, Texas, USA) (A. J. Hu and A. K. Martin, eds.), Lecture Notes in Computer Science, vol. 3312, Springer-Verlag, Berlin, 2004, pp. 21–36.

[DHR05] L. Doyen, T. A. Henzinger, and J.-F. Raskin, *Automatic rectangular refinement of affine hybrid systems*, Tech. Report 2005.47, Centre Fédéré en Vérification, Université Libre de Bruxelles, Belgium, 2005.

[Dil89] D. L. Dill, *Timing assumptions and verification of finite-state concurrent systems*, Proceedings of the International Workshop on Automatic Verification Methods for Finite State Systems (Grenoble, France) (J. Sifakis, ed.), Lecture Notes in Computer Science, vol. 407, Springer-Verlag, Berlin, 1989, pp. 197–212.

[DM05] D. Doose and Z. Mammeri, *Polyhedra-based approach for incremental validation of real-time systems*, Proceedings of the International Conference on Embedded and Ubiquitous Computing (EUC 2005) (Nagasaki, Japan) (L. T. Yang, M. Amamiya, Z. Liu, M. Guo, and F. J. Rammig, eds.), Lecture Notes in Computer Science, vol. 3824, Springer-Verlag, Berlin, 2005, pp. 184–193.

[DP99] G. Delzanno and A. Podelski, *Model checking in CLP*, Tools and Algorithms for Construction and Analysis of Systems, 5th International Conference, TACAS '99 (Amsterdam, The Netherlands) (R. Cleaveland, ed.), Lecture Notes in Computer Science, vol. 1579, Springer-Verlag, Berlin, 1999, pp. 223–239.

[DRS01] N. Dor, M. Rodeh, and S. Sagiv, *Cleanness checking of string manipulations in C programs via integer analysis*, Static Analysis: 8th International Symposium, SAS 2001 (Paris, France) (P. Cousot, ed.), Lecture Notes in Computer Science, vol. 2126, Springer-Verlag, Berlin, 2001, pp. 194–212.

[Ell04] R. Ellenbogen, *Fully automatic verification of absence of errors via interprocedural integer analysis*, Master's thesis, School of Computer Science, Tel-Aviv University, Tel-Aviv, Israel, December 2004.

[FHK04] G. Frehse, Z. Han, and B. Krogh, *Assume-guarantee reasoning for hybrid I/O-automata by over-approximation of continuous interaction*, Proceedings of the 43rd IEEE Conference on Decision and Control (CDC 2004) (Atlantis, Paradise Island, Bahamas), 2004.

[FKR06] G. Frehse, B. H. Krogh, and R. A. Rutenbar, *Verifying analog oscillator circuits using forward/backward refinement*, Proceedings of the 9th Conference on Design, Automation and Test in Europe (DATE 06) (Munich, Germany), ACM SIGDA, 2006, CD-ROM publication.

[FKRM06] G. Frehse, B. H. Krogh, R. A. Rutenbar, and O. Maler, *Time domain verification of oscillator circuit properties*, Proceedings of the First Workshop on Formal Verification of Analog Circuits (FAC 2005) (Edinburgh, Scotland), vol. 153, Electronic Notes in Theoretical Computer Science, no. 3, Elsevier Science B.V., 2006, pp. 9–22.

[FP96] K. Fukuda and A. Prodon, *Double description method revisited*, Combinatorics and Computer Science, 8th Franco-Japanese and 4th Franco-Chinese Conference, Brest, France, July 3-5, 1995, Selected Papers (M. Deza, R. Euler, and Y. Manoussakis, eds.), Lecture Notes in Computer Science, vol. 1120, Springer-Verlag, Berlin, 1996, pp. 91–111.

[Fre04] G. Frehse, *Compositional verification of hybrid systems with discrete interaction using simulation relations*, Proceedings of the IEEE Conference on Computer Aided Control Systems Design (CACSD 2004) (Taipei, Taiwan), 2004.

[Fre05] ______, *PHAVer: Algorithmic verification of hybrid systems past HyTech*, Hybrid Systems: Computation and Control: Proceedings of the 8th International Workshop (HSCC 2005) (Zürich, Switzerland) (M. Morari and L. Thiele, eds.), Lecture Notes in Computer Science, vol. 3414, Springer-Verlag, Berlin, 2005, pp. 258–273.

[GKR04] S. Gupta, B. H. Krogh, and R. A. Rutenbar, *Towards formal verification of analog designs*, Proceedings of the 2004 International Conference on Computer-Aided Design (San Jose, CA, USA), IEEE Computer Society / ACM, 2004, pp. 210–217.

[GR06] B. S. Gulavani and S. K. Rajamani, *Counterexample driven refinement for abstract interpretation*, Proceedings of the 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2006) (Vienna, Austria) (H. Hermanns and J. Palsberg, eds.), Lecture Notes in Computer Science, vol. 3920, Springer-Verlag, Berlin, 2006, pp. 474–488.

[Gra91] P. Granger, *Static analysis of linear congruence equalities among variables of a program*, TAPSOFT'91: Proceedings of the International Joint Conference on Theory and Practice of Software Development, Volume 1: Colloquium on Trees in Algebra and Programming (CAAP'91) (Brighton, UK) (S. Abramsky and T. S. E. Maibaum, eds.), Lecture Notes in Computer Science, vol. 493, Springer-Verlag, Berlin, 1991, pp. 169–192.

[Gra92] ———, *Improving the results of static analyses programs by local decreasing iteration*, Proceedings of the 12th Conference on Foundations of Software Technology and Theoretical Computer Science (New Delhi, India) (R. K. Shyamasundar, ed.), Lecture Notes in Computer Science, vol. 652, Springer-Verlag, Berlin, 1992, pp. 68–79.

[Gra97] ———, *Static analyses of congruence properties on rational numbers (extended abstract)*, Static Analysis: Proceedings of the 4th International Symposium (Paris, France) (P. Van Hentenryck, ed.), Lecture Notes in Computer Science, vol. 1302, Springer-Verlag, Berlin, 1997, pp. 278–292.

[GRS05] D. Gopan, T. W. Reps, and M. Sagiv, *A framework for numeric analysis of array operations*, Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (Long Beach, California, USA), 2005, pp. 338–350.

[Hal79] N. Halbwachs, *Détermination automatique de relations linéaires vérifiées par les variables d'un programme*, Thèse de 3ème cycle d'informatique, Université scientifique et médicale de Grenoble, Grenoble, France, March 1979.

[Hal93] ———, *Delay analysis in synchronous programs*, Computer Aided Verification: Proceedings of the 5th International Conference (Elounda, Greece) (C. Courcoubetis, ed.), Lecture Notes in Computer Science, vol. 697, Springer-Verlag, Berlin, 1993, pp. 333–346.

[Hen96] T. A. Henzinger, *The theory of hybrid automata*, Proceedings of the 11th Annual Symposium on Logic in Computer Science (LICS), IEEE Computer Society Press, 1996, pp. 278–292.

[HH95a] T. A. Henzinger and P.-H. Ho, *Algorithmic analysis of nonlinear hybrid systems*, Computer Aided Verification: Proceedings of the 7th International Conference (Liège, Belgium) (P. Wolper, ed.), Lecture Notes in Computer Science, vol. 939, Springer-Verlag, Berlin, 1995, pp. 225–238.

[HH95b] ———, *A note on abstract interpretation strategies for hybrid automata*, Hybrid Systems II (P. J. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, eds.), Lecture Notes in Computer Science, vol. 999, Springer-Verlag, Berlin, 1995, pp. 252–264.

[HHB02] W. Hartong, L. Hedrich, and E. Barke, *On discrete modeling and model checking for nonlinear analog systems*, Computer Aided Verification: Proceedings of the 14th International Conference (Copenhagen, Denmark) (E. Brinksma and K. G. Larsen, eds.), Lecture Notes in Computer Science, vol. 2404, Springer-Verlag, Berlin, 2002, pp. 401–413.

[HHWT97] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi, HyTech*: A model checker for hybrid systems*, Software Tools for Technology Transfer **1** (1997), no. 1+2, 110–122.

[HMG06] N. Halbwachs, D. Merchat, and L. Gonnord, *Some ways to reduce the space dimension in polyhedra computations*, Formal Methods in System Design **29** (2006), no. 1, 79–95.

[HMPV03] N. Halbwachs, D. Merchat, and C. Parent-Vigouroux, *Cartesian factoring of polyhedra in linear relation analysis*, Static Analysis: Proceedings of the 10th International Symposium (San Diego, California, USA) (R. Cousot, ed.), Lecture Notes in Computer Science, vol. 2694, Springer-Verlag, Berlin, 2003, pp. 355–365.

[HPR94] N. Halbwachs, Y.-E. Proy, and P. Raymond, *Verification of linear hybrid systems by means of convex approximations*, Static Analysis: Proceedings of the 1st International Symposium (Namur, Belgium) (B. Le Charlier, ed.), Lecture Notes in Computer Science, vol. 864, Springer-Verlag, Berlin, 1994, pp. 223–237.

[HPR97] N. Halbwachs, Y.-E. Proy, and P. Roumanoff, *Verification of real-time systems using linear relation analysis*, Formal Methods in System Design **11** (1997), no. 2, 157–185.

[HPWT01] T. A. Henzinger, J. Preussig, and H. Wong-Toi, *Some lessons from the* HYTECH *experience*, Proceedings of the 40th Annual Conference on Decision and Control, IEEE Computer Society Press, 2001, pp. 2887–2892.

[HU04] C. Hymans and E. Upton, *Static analysis of gated data dependence graphs*, Static Analysis: Proceedings of the 11th International Symposium (Verona, Italy) (R. Giacobazzi, ed.), Lecture Notes in Computer Science, vol. 3148, Springer-Verlag, Berlin, 2004, pp. 197–211.

[Kah87] G. Kahn, *Natural semantics*, Proceedings of the 4th Annual Symposium on Theoretical Aspects of Computer Science (Passau, Germany) (F.-J. Brandenburg, G. Vidal-Naquet, and M. Wirsing, eds.), Lecture Notes in Computer Science, vol. 247, Springer-Verlag, Berlin, 1987, pp. 22–39.

[Kar76] M. Karr, *Affine relationships among variables of a program*, Acta Informatica **6** (1976), 133–151.

[KKM+05] C. Kruegel, E. Kirda, D. Mutz, W. Robertson, and G. Vigna, *Automating mimicry attacks using static binary analysis*, Proceedings of Security '05, the 14th USENIX Security Symposium (Baltimore, MD, USA), 2005, pp. 161–176.

[KM06] K. Krishnan and J.E. Mitchell, *A unifying framework for several cutting plane methods for semidefinite programming*, Optimization Methods and Software **21** (2006), no. 1, 57–74.

[Le 92] H. Le Verge, *A note on Chernikova's algorithm*, *Publication interne* 635, IRISA, Campus de Beaulieu, Rennes, France, 1992.

[Ler06] X. Leroy, *Coinductive big-step operational semantics*, Programming Languages and Systems, Proceedings of the 14th European Symposium on Programming (Vienna, Austria) (P. Sestoft, ed.), Lecture Notes in Computer Science, vol. 3924, Springer-Verlag, Berlin, 2006, pp. 54–68.

[LLPY97] K. Larsen, F. Larsson, P. Pettersson, and W. Yi, *Efficient verification of real-time systems: Compact data structure and state-space reduction*, Proceedings of the 18th IEEE Real-Time Systems Symposium (RTSS'97) (San Francisco, CA), IEEE Computer Society Press, 1997, pp. 14–24.

[LM92] J.-L. Lassez and M. J. Maher, *On Fourier's algorithm for linear arithmetic constraints*, J. Autom. Reasoning **9** (1992), no. 3, 373–379.

[Loe99] V. Loechner, *PolyLib: A library for manipulating parameterized polyhedra*. Available at `http://icps.u-strasbg.fr/~loechner/polylib/`, March 1999, Declares itself to be a continuation of [Wil93].

[Mal06] O. Maler, *Analog circuit verification: A state of an art*, Proceedings of the First Workshop on Formal Verification of Analog Circuits (FAC 2005) (Edinburgh, Scotland), vol. 153, Electronic Notes in Theoretical Computer Science, no. 3, Elsevier Science B.V., 2006, pp. 3–7.

[MB05] F. Mesnard and R. Bagnara, *cTI: A constraint-based termination inference tool for ISO-Prolog*, Theory and Practice of Logic Programming **5** (2005), no. 1&2, 243–257.

[Min01] A. Miné, *The octagon abstract domain*, Proceedings of the Eighth Working Conference on Reverse Engineering (WCRE'01) (Stuttgart, Germany), IEEE Computer Society Press, 2001, pp. 310–319.

[Min05] ———, *Weakly relational numerical abstract domains*, Ph.D. thesis, École Polytechnique, Paris, France, March 2005.

[MRTT53] T. S. Motzkin, H. Raiffa, G. L. Thompson, and R. M. Thrall, *The double description method*, Contributions to the Theory of Games – Volume II (H. W. Kuhn and A. W. Tucker, eds.), Annals of Mathematics Studies, no. 28, Princeton University Press, Princeton, New Jersey, 1953, pp. 51–73.

[MS00] O. Müller and T. Stauner, *Modelling and verification using linear hybrid systems*, Mathematical and Computer Modelling of Dynamical Systems **6** (2000), no. 1, 71–89.

[MS04] M. Müller-Olm and H. Seidl, *A note on Karr's algorithm*, Automata, Languages and Programming: Proceedings of the 31st International Colloquium (ICALP 2004) (Turku, Finland) (J. Diaz, J. Karhumäki, and A. Lepistö et al., eds.), Lecture Notes in Computer Science, vol. 3142, Springer-Verlag, Berlin, 2004, pp. 1016–1028.

[NJPF99] T. Nakanishi, K. Joe, C. D. Polychronopoulos, and A. Fukuda, *The modulo interval: A simple and practical representation for program analysis*, Proceedings of the

1999 International Conference on Parallel Architectures and Compilation Techniques (Newport Beach, California, USA), IEEE Computer Society, 1999, pp. 91–96.

[NR00] S. P. K. Nookala and T. Risset, *A library for Z-polyhedral operations*, *Publication interne* 1330, IRISA, Campus de Beaulieu, Rennes, France, 2000.

[Plo81] G. Plotkin, *A structural approach to operational semantics*, Tech. Report DAIMI FN-19, Computer Science Department, University of Aarhus, Denmark, 1981.

[QRR96] P. Quinton, S. Rajopadhye, and T. Risset, *On manipulating Z-polyhedra*, Tech. Report 1016, IRISA, Campus Universitaire de Bealieu, Rennes, France, July 1996.

[Sch95] D. A. Schmidt, *Natural-semantics-based abstract interpretation (preliminary version)*, Static Analysis: Proceedings of the 2nd International Symposium (Glasgow, UK) (A. Mycroft, ed.), Lecture Notes in Computer Science, vol. 983, Springer-Verlag, Berlin, 1995, pp. 1–18.

[Sch97] ———, *Abstract interpretation of small-step semantics*, Analysis and Verification of Multiple-Agent Languages (M. Dam, ed.), Lecture Notes in Computer Science, vol. 1192, Springer-Verlag, Berlin, 1997, 5th LOMAPS Workshop Stockholm, Sweden, June 24–26, 1996, Selected Papers, pp. 76–99.

[Sch98] ———, *Trace-based abstract interpretation of operational semantics*, LISP and Symbolic Computation **10** (1998), no. 3, 237–271.

[Sch99] A. Schrijver, *Theory of linear and integer programming*, Wiley Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 1999.

[SCR06] H. Song, K. J. Compton, and W. C. Rounds, *SPHIN: a model checker for reconfigurable hybrid systems based on SPIN*, Proceedings of the 5th International Workshop on Automated Verification of Critical Systems (University of Warwick, UK) (R. Lazic and R. Nagarajan, eds.), Electronic Notes in Theoretical Computer Science, vol. 145, 2006, pp. 167–183.

[SCSM06] S. Sankaranarayanan, M. Colón, H. B. Sipma, and Z. Manna, *Efficient strongly relational polyhedral analysis*, Verification, Model Checking and Abstract Interpretation: Proceedings of the 7th International Conference (VMCAI 2006) (Charleston, SC, USA) (E. A. Emerson and K. S. Namjoshi, eds.), Lecture Notes in Computer Science, vol. 3855, Springer-Verlag, Berlin, 2006, pp. 111–125.

[SKH02] A. Simon, A. King, and J. M. Howe, *Two variables per linear inequality as an abstract domain*, Logic Based Program Synthesis and Tranformation, 12th International Workshop (Madrid, Spain) (M. Leuschel, ed.), Lecture Notes in Computer Science, vol. 2664, Springer-Verlag, Berlin, 2002, pp. 71–89.

[SKS00] R. Shaham, E. K. Kolodner, and S. Sagiv, *Automatic removal of array memory leaks in Java*, Proceedings of the 9th International Conference on Compiler Construction (CC 2000) (Berlin, Germany) (D. A. Watt, ed.), Lecture Notes in Computer Science, vol. 1781, Springer-Verlag, Berlin, 2000, pp. 50–66.

[SSM05] S. Sankaranarayanan, H. B. Sipma, and Z. Manna, *Scalable analysis of linear systems using mathematical programming*, Verification, Model Checking and Abstract Interpretation: Proceedings of the 6th International Conference (VMCAI 2005) (Paris, France) (R. Cousot, ed.), Lecture Notes in Computer Science, vol. 3385, Springer-Verlag, Berlin, 2005, pp. 25–41.

[SSM06] ———, *Fixed point iteration for computing the time elapse operator*, Hybrid Systems: Computation and Control: Proceedings of the 9th International Workshop (HSCC 2006) (Santa Barbara, CA, USA) (J. Hespanha and A. Tiwari, eds.), Lecture Notes in Computer Science, vol. 3927, Springer-Verlag, Berlin, 2006, pp. 537–551.

[SV91] K. Sohn and A. Van Gelder, *Termination detection in logic programs using argument sizes*, Proceedings of the Tenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems (Denver, Colorado), Association for Computing Machinery, 1991, Extended abstract., pp. 216–226.

[SW70] J. Stoer and C. Witzgall, *Convexity and optimization in finite dimensions I*, Springer-Verlag, Berlin, 1970.

[VB04] A. Venet and G. Brat, *Precise and efficient static array bound checking for large embedded C programs*, Proceedings of the ACM SIGPLAN 2004 Conference on Programming Language Design and Implementation (PLDI'04) (Washington, DC, USA), ACM Press, 2004, pp. 231–242.

[vOSV06] K. van Hee, O. Oanea, N. Sidorova, and M. Voorhoeve, *Verifying generalized soundness for workflow nets*, Perspectives of System Informatics: Proceedings of the Sixth International Andrei Ershov Memorial Conference (Akademgorodok, Novosibirsk, Russia) (I. Virbitskaite and A. Voronkov, eds.), Lecture Notes in Computer Science, vol. 4378, Springer-Verlag, Berlin, 2006, pp. 231–244.

[Wil93] D. K. Wilde, *A library for doing polyhedral operations*, Master's thesis, Oregon State University, Corvallis, Oregon, December 1993, Also published as IRISA *Publication interne* 785, Rennes, France, 1993.

Department of Mathematics, University of Parma, Italy
E-mail address: `bagnara@cs.unipr.it`

School of Computing, University of Leeds, UK
E-mail address: `hill@comp.leeds.ac.uk`

Department of Mathematics, University of Parma, Italy
E-mail address: `zaffanella@cs.unipr.it`