Dynamic interval analysis by abstract interpretation*

Patrick Cousot[1][0000−0003−0101−9953]

CS, CIMS, NYU, New York, NY, USA, pcousot@cims.nyu.edu, visiting IMDEA Software, Madrid, Spain

Dedicated to Klaus Havelund for his 65th birthday

Abstract. Interval arithmetic introduced by Ramon E. Moore in scientific computing to put bounds on rounding errors in floating point computations was a very first example of dynamic program analysis. We show that it can be formalized by abstract interpretation.

Keywords: Abstract interpretation · Dynamic analysis · Interval Arithmetics · Soundness.

1 Introduction

Ramon E. Moore [31,32,33] may have introduced the first dynamic analysis ever to put bounds on rounding (or roundoff) errors in floating point computations [24,37]. Similar to static analyses, this can be formalized and proved sound (but incomplete) by abstract interpretation [6,8].

Given the formal structural trace semantics of a C-subset on reals, the interval abstraction provides the best abstraction of these execution traces on reals into execution traces on float intervals. Unfortunately, this best interval abstraction is not implementable since it is not inductive and requires computations on reals to guarantee that the interval abstraction is the best possible (i.e. the float intervals are the smallest possible that include the real computation).

By calculus, we design a formal structural trace semantics of this C-subset on float interval which over-approximates the best abstraction of real traces into float interval traces. All computations on reals are over-approximated by performing the computation on two ends of an interval [l, h] where l and h are floating point numbers so that this abstract interval semantics is implementable. For tests and loops both true and false alternatives may be taken while only one would be taken with reals. Although incomplete and sometimes imprecise, this is sound.

The difference with dynamic analysis [21] is that, interval arithmetics collects interval information about real executions but does not check this collected information for a specification. Instead, it is used to replace the real computation. But

* Supported by NSF Grant CCF-1617717.

the formalization by abstract interpretation is exactly the same. As discussed in the conclusion, abstraction is used to relate the original and the instrumented semantics as well as the instrumented semantics and the specification and so the original semantics and the specification via a monitor [5].

2 Syntax and Trace Semantics of the Programming Language

Syntax Programs are a subset of `C` with the following context-free syntax.

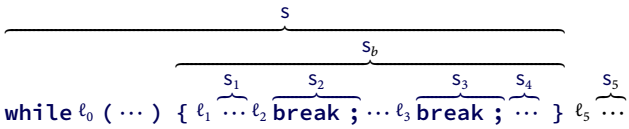
$\mathtt{x}, \mathtt{y}, \ldots \in \mathbb{X}$		variable ($\mathbb{X}$ not empty)
$\mathtt{A} \in \mathbb{A}$	::= `0.1` | `x` | $\mathtt{A}_1$ `-` $\mathtt{A}_2$	arithmetic expression
$\mathtt{B} \in \mathbb{B}$	::= $\mathtt{A}_1$ `<` $\mathtt{A}_2$ | $\mathtt{B}_1$ `nand` $\mathtt{B}_2$	boolean expression
$\mathtt{S} \in \mathbb{S}$	::=	statement
	`x = A ;`	assignment
	`;`	skip
	`if (B) S` | `if (B) S else S`	conditionals
	`while (B) S` | `break ;`	iteration and break
	`{ Sl }`	compound statement
$\mathtt{Sl} \in \mathbb{S}\mathbb{l}$	::= `Sl S` | ϵ	statement list
$\mathtt{P} \in \mathbb{P}$	::= `Sl`	program

The float constant `0.1` is $0.000(1100)^\infty$ in binary so has no exact finite binary representation. It is approximated as $0.1.000000014901161193847656250 0\ldots$. A break exits the closest enclosing loop, if none this is a syntactic error. If `P` is a program then `int main (void) { P }` is a valid `C` program (after adding variable declarations that we omit for concision). We call "[program] component" $\mathtt{S} \in \mathbb{P}\mathtt{c} \triangleq \mathbb{S} \cup \mathbb{S}\mathbb{l} \cup \mathbb{P}$ either a statement, a statement list, or a program. We let $\lhd$ be the syntactic relation between immediate syntactic components. For example, if $\mathtt{S} = \mathtt{if\ (B)\ S}_t\ \mathtt{else\ S}_f$ then $\mathtt{B} \lhd \mathtt{S}$, $\mathtt{S}_t \lhd \mathtt{S}$, and $\mathtt{S}_f \lhd \mathtt{S}$.

Program labels Labels $\ell \in \mathbb{L}$ are not part of the language, but useful to discuss program points reached during execution. For each program component `S`, we define

at⟦S⟧	the program point at which execution of `S` starts;
aft⟦S⟧	the program exit point after `S`, at which execution of `S` is supposed to normally terminate, if ever;
esc⟦S⟧	a boolean indicating whether or not the program component `S` contains a `break ;` statement escaping out of that component `S`;
brk-to⟦S⟧	the program point at which execution of the program component `S` goes to when a `break ;` statement escapes out of that component `S`;
brks-of⟦S⟧	the set of labels of all `break ;` statements that can escape out of `S`;
in⟦S⟧	the set of program points inside `S` (including at⟦S⟧ but excluding aft⟦S⟧ and brk-to⟦S⟧);
labs⟦S⟧	the potentially reachable program points while executing `S` either at, in, or after the statement, or resulting from a break.

Here is an example,



$\ell_0 = \mathsf{at}[\![\mathsf{S}]\!] = \mathsf{aft}[\![\mathsf{S}_4]\!]$, $\ell_1 = \mathsf{at}[\![\mathsf{S}_1]\!] = \mathsf{at}[\![\mathsf{S}_b]\!]$, $\ell_2 = \mathsf{at}[\![\mathsf{S}_2]\!] = \mathsf{aft}[\![\mathsf{S}_1]\!]$, $\ell_3 = \mathsf{at}[\![\mathsf{S}_3]\!]$,
$\ell_5 = \mathsf{at}[\![\mathsf{S}_5]\!] = \mathsf{brk\text{-}to}[\![\mathsf{S}_b]\!] = \mathsf{aft}[\![\mathsf{S}]\!]$, $\mathsf{esc}[\![\mathsf{S}_b]\!] = \mathtt{tt}$, $\mathsf{brks\text{-}of}[\![\mathsf{S}_b]\!] = \{\ell_2, \ell_3\}$, $\mathsf{esc}[\![\mathsf{S}]\!] = \mathtt{ff}$,
$\mathsf{in}[\![\mathsf{S}_b]\!] = \{\ell_1, \ldots, \ell_2, \ldots, \ell_3, \ldots\}$, $\mathsf{in}[\![\mathsf{S}]\!] = \mathsf{labs}[\![\mathsf{S}_b]\!] = \{\ell_0, \ell_1, \ldots, \ell_2, \ldots, \ell_3, \ldots\}$,
$\mathsf{labs}[\![\mathsf{S}]\!] = \{\ell_0, \ell_1, \ldots, \ell_2, \ldots, \ell_3, \ldots, \ell_5\}$

Float intervals Let $\mathbb{F}$[1] be the set of floating point numbers (including $-\infty$ and $+\infty$, but excluding NaN (Not a Number)[2] and -0, $+0$[3]). The float intervals are

$$\mathbb{I} \triangleq \bigcup \begin{array}{l} \{\varnothing\} \cup \{[\underline{x}, \overline{x}] \mid \underline{x}, \overline{x} \in \mathbb{F} \setminus \{-\infty, +\infty\} \wedge \underline{x} \leqslant \overline{x}\} \\ \{[-\infty, \overline{x}] \mid \overline{x} \in \mathbb{F} \setminus \{-\infty\}\} \cup \{[\underline{x}, +\infty] \mid \underline{x} \in \mathbb{F} \setminus \{+\infty\}\} \end{array}$$

with the empty interval $\varnothing$ and the intervals $[-\infty, -\infty] \notin \mathbb{I}$ and $[\infty, \infty] \notin \mathbb{I}$ are excluded.

The order on intervals is $\varnothing \sqsubseteq^i \varnothing \sqsubseteq^i [\underline{x}, \overline{x}] \sqsubseteq^i [\underline{y}, \overline{y}]$ if and only if $\underline{y} \leqslant \underline{x} \leqslant \overline{x} \leqslant \overline{y}$. We have the complete lattice $\langle \mathbb{I}, \sqsubseteq^i, \varnothing, [-\infty, +\infty], \bigsqcap^i, \bigsqcup^i \rangle$.

Values Programs compute on values $\mathbb{V}$. Values can be reals $\mathbb{R}$, floating point numbers ($\mathbb{F} \setminus \{\mathsf{NaN}, -0, +0\}) \cup \{0\}$[4]), or float intervals $\mathbb{I}$. For simplicity, we assume that execution stops in case of error (*e.g.* when dividing by zero).

Traces A trace π is a non-empty sequence of states where states $\langle \ell, \rho \rangle \in \mathbb{S}_{\mathbb{V}} \triangleq (\mathbb{L} \times \mathbb{E}\mathsf{nv}_{\mathbb{V}})$ are pairs of a program label $\ell \in \mathbb{L}$ designating the next action to be executed in the program and an environment $\rho \in \mathbb{E}\mathsf{nv}_{\mathbb{V}} \triangleq \mathbb{X} \to \mathbb{V}$ assigning values $\rho(\mathsf{x}) \in \mathbb{V}$ to variables $\mathsf{x} \in \mathbb{X}$. A trace π can be finite $\pi \in \mathbb{S}^+_{\mathbb{V}}$ or infinite $\pi \in \mathbb{S}^\infty_{\mathbb{V}}$ (recording a non-terminating computation) so $\mathbb{S}^{+\infty}_{\mathbb{V}} \triangleq \mathbb{S}^+_{\mathbb{V}} \cup \mathbb{S}^\infty_{\mathbb{V}}$. We let $|\pi| = n \in \mathbb{N}_*$ be the length of a finite trace $\pi = \bigfrown_{i=0}^{n-1} \pi_i = \pi_0 \ldots \pi_{n-1} \in \mathbb{S}^+_{\mathbb{V}}$ and $|\pi| = \infty$ for infinite traces $\pi = \bigfrown_{i \in \mathbb{N}} \pi_i = \pi_0 \ldots \pi_n \ldots \in \mathbb{S}^\infty_{\mathbb{V}}$. Trace concatenation $\frown$ is defined as follows

[1] For simplicity, we consider only one category of floats say of type `float` in C, ignoring `double`, `long double`, *etc.*

[2] For simplicity, we ignore NaN and assume that execution stops in case a NaN would be returned when executing an expression.

[3] For simplicity, we ignore -0, $+0$ used to determine whether $+\infty$ or $-\infty$ is returned when dividing a nonzero number by a zero.

[4] Therefore $+0 = -0 = 0$ and 0 is positive for the rule of signs

$\pi_1\sigma_1 \frown \sigma_2\pi_2$ undefined if $\sigma_1 \neq \sigma_2$
$\pi_1\sigma_1 \frown \sigma_1\pi_2 \triangleq \pi_1\sigma_1\pi_2$ if $\pi_1 \in \mathbb{S}^+_{\mathbb{V}}$ is finite
$\pi_1 \frown \sigma_2\pi_2 \triangleq \pi_1$ if $\pi_1 \in \mathbb{S}^\infty_{\mathbb{V}}$ is infinite

In pattern matching, we sometimes need the empty trace $\ni$. For example the match $\sigma\pi\sigma' = \sigma$ holds when $\pi = \ni$ and $\sigma = \sigma'$.

Formal definition of the real and float prefix trace semantics The prefix trace semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ for reals $\mathbb{V} = \mathbb{R}$ or float $\mathbb{V} = \mathbb{F}$ is defined below. The definition is structural (by induction on the syntax) using fixpoints for the iteration. $\boldsymbol{\mathcal{S}}^*_{\mathbb{R}}[\![\mathtt{S}]\!]$ and $\boldsymbol{\mathcal{S}}^*_{\mathbb{F}}[\![\mathtt{S}]\!]$ will be abstracted in the prefix trace interval semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathtt{S}]\!]$ in Section **7**.

- *The value of an arithmetic expression* A in environment $\rho \in \mathbb{E}\mathtt{nv}_{\mathbb{V}} \triangleq \mathbb{X} \to \mathbb{V}$ is $\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho \in \mathbb{V}$:

$$\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{0.1}]\!]\rho \triangleq 0.1_{\mathbb{V}} \quad \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{x}]\!]\rho \triangleq \rho(\mathtt{x}) \quad \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\rho \triangleq \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho -_{\mathbb{V}} \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho \quad (1)$$

where $0.1_{\mathbb{V}}$ denotes the real 0.1 and $-_{\mathbb{V}}$ the difference in $\mathbb{V}$. For example $-_{\mathbb{F}}$ is the difference found on IEEE-754 machines and must take rounding mode (and the machine specificities [30]) into account.

- *The prefix traces of an assignment statement* $\mathtt{S} ::= \ell\ \mathtt{x = A\ ;}$ (where $\mathtt{at}[\![\mathtt{S}]\!] = \ell$) either stops in an initial state $\langle \ell,\ \rho\rangle$ or is this initial state $\langle \ell,\ \rho\rangle$ followed by the next state $\langle \mathtt{aft}[\![\mathtt{S}]\!],\ \rho[\mathtt{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho]\rangle$ recording the assignment of the value $\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho$ of the arithmetic expression to variable x when reaching the label $\mathtt{aft}[\![\mathtt{S}]\!]$ after the assignment[5].

$$\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!] = \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathtt{nv}_{\mathbb{V}}\} \cup \{\langle \ell,\ \rho\rangle\langle \mathtt{aft}[\![\mathtt{S}]\!],\ \rho[\mathtt{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathtt{nv}_{\mathbb{V}}\} \quad (2)$$

- *The prefix trace semantics of a break statement* $\mathtt{S} ::= \ell\ \mathtt{break\ ;}$ either stops at ℓ or goes on to the break label $\mathtt{brk\text{-}to}[\![\mathtt{S}]\!]$ (which is defined syntactically as the exit label of the closest enclosing iteration).

$$\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!] \triangleq \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathtt{nv}_{\mathbb{V}}\} \cup \{\langle \ell,\ \rho\rangle\langle \mathtt{brk\text{-}to}[\![\mathtt{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathtt{nv}_{\mathbb{V}}\} \quad (3)$$

- *The value of an boolean expression* B in environment ρ is the boolean $\boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho \in \mathbb{B} \triangleq \{\mathtt{tt}, \mathtt{ff}\}$:

$$\boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathtt{A}_1 < \mathtt{A}_2]\!]\rho \triangleq \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho < \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho \quad (4)$$
$$\boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathtt{B}_1\ \mathtt{nand}\ \mathtt{B}_2]\!]\rho \triangleq \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathtt{B}_1]\!]\rho \uparrow \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathtt{B}_2]\!]\rho$$

where $<$ is strictly less than on reals and floats while $\uparrow$ is the "not and" boolean operator.

- *The prefix trace semantics of a conditional statement* $\mathtt{S} ::= \mathtt{if}\ \ell\ \mathtt{(B)}\ \mathtt{S}_t$ is
  - either the trace $\langle \ell,\ \rho\rangle$ when the observation of the execution stops on entry $\ell = \mathtt{at}[\![\mathtt{S}]\!]$ of the program component S for initial environment ρ;

[5] If we had NaNs and $\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho$ returns a NaN, the second term would include a condition $\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho \neq \mathtt{NaN}$ to terminate execution on error.

- or, when the value of the boolean expression $\mathtt{B}$ for ρ is false $\mathtt{ff}$, the initial state $\langle \ell, \rho\rangle$ followed by the state $\langle \mathsf{aft}[\![\mathtt{S}]\!], \rho\rangle$ at the label $\mathsf{aft}[\![\mathtt{S}]\!]$ after the conditional statement;
- or finally, when the value of the boolean expression $\mathtt{B}$ for ρ is true $\mathtt{tt}$, the initial state$\langle \ell, \rho\rangle$ followed by a prefix trace of $\mathtt{S}_t$ starting $\mathsf{at}[\![\mathtt{S}_t]\!]$ in environment ρ (and possibly ending $\mathsf{aft}[\![\mathtt{S}_t]\!] = \mathsf{aft}[\![\mathtt{S}]\!]$).

$$\begin{aligned}\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!] \triangleq \quad & \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathsf{nv}_{\mathbb{V}}\} \cup \{\langle \ell,\ \rho\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!],\ \rho\rangle \mid \mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{ff}\} \\ & \cup \{\langle \ell,\ \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \rho\rangle\pi \mid \mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \rho\rangle\pi \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}_t]\!]\}\end{aligned} \tag{5}$$

Observe that definition (5) includes the case of termination of the true branch $\mathtt{S}_t$ and so also of termination of the conditional $\mathtt{S}$ since $\mathsf{aft}[\![\mathtt{S}]\!] = \mathsf{aft}[\![\mathtt{S}_t]\!]$. Moreover, if the conditional $\mathtt{S}$ is within an iteration and contains a break statement in the true branch $\mathtt{S}_t$ then $\mathsf{brk\text{-}to}[\![\mathtt{S}]\!] = \mathsf{brk\text{-}to}[\![\mathtt{S}_t]\!]$, so from $\langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \rho\rangle\pi\langle \mathsf{brk\text{-}to}[\![\mathtt{S}_t]\!],\ \rho'\rangle \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}_t]\!]$ and $\mathscr{B}[\![\mathtt{B}]\!]\rho = \mathtt{tt}$, we infer that $\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \rho\rangle\pi\langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!],\ \rho'\rangle \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$.

- *The prefix trace semantics of the empty statement list* $\mathtt{Sl} = \epsilon$ is reduced to the states at that empty statement (which is also after that empty statement since $\mathsf{at}[\![\mathtt{Sl}]\!] = \mathsf{aft}[\![\mathtt{Sl}]\!]$).

$$\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}]\!] \triangleq \{\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathsf{nv}_{\mathbb{V}}\} \tag{6}$$

- The prefix traces of the *prefix trace semantics of a non-empty statement list* $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$ are the prefix traces of $\mathtt{Sl}'$ or the finite maximal traces of $\mathtt{Sl}'$ followed by a prefix trace of $\mathtt{S}$.

$$\begin{aligned}&\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}]\!] \triangleq \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!] \cup \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!] \frown \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!] \\ &\mathscr{S} \frown \mathscr{S}' \triangleq \{\pi \frown \pi' \mid \pi \in \mathscr{S} \wedge \pi' \in \mathscr{S}' \wedge \pi \frown \pi' \text{ is well-defined}\}\end{aligned} \tag{7}$$

Notice that if $\pi \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!]$, $\pi' \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$, and $\pi \frown \pi' \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}]\!]$ then the last state of π must be the first state of π' and this state is $\mathsf{at}[\![\mathtt{S}]\!] = \mathsf{aft}[\![\mathtt{Sl}']\!]$ and so the trace π must be a maximal terminating execution of $\mathtt{Sl}'$ *i.e.* $\mathtt{S}$ is executed if and only if $\mathtt{Sl}'$ terminates.

- *The prefix finite trace semantic definition* $\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ (8) *of an iteration statement of the form* $\mathtt{S} ::= \mathtt{while}\ ^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$ where $\ell = \mathsf{at}[\![\mathtt{S}]\!]$ is the $\subseteq$-least solution $\mathsf{lfp}^{\subseteq}\ \mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ to the equation $X = \mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!](X)$. Since $\mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!] \in \wp(\mathbb{S}^+) \to \wp(\mathbb{S}^+)$ is $\subseteq$-monotone (if $X \subseteq X'$ then $\mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!](X) \subseteq \mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!](X')$ and $\langle \wp(\mathbb{S}^+), \subseteq, \varnothing, \mathbb{S}^+, \cup, \cap\rangle$ is a complete lattice, $\mathsf{lfp}^{\subseteq}\ \mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ exists by Tarski's fixpoint theorem and can be defined as the limit of iterates [7]. In definition (8) of the transformer $\mathscr{F}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$, case (8.a) corresponds to a loop execution observation stopping on entry, (8.b) corresponds to an observation of a loop exiting after 0 or more iterations, and (8.c) corresponds to a loop execution observation that stops anywhere in the body $\mathtt{S}_b$ after 0 or more iterations. This last case covers the case of an iteration terminated by a break statement (to $\mathsf{aft}[\![\mathtt{S}]\!]$ after the iteration statement). This last case also covers the case of termination of the loop body $\mathtt{S}_b$ at label $\mathsf{aft}[\![\mathtt{S}_b]\!] = \mathsf{at}[\![\mathtt{while}\ ^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!] = \ell$ so that the iteration goes on.

$$\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{while}\ ^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!] = \mathsf{lfp}^{\subseteq}\ \mathscr{F}^*_{\mathbb{V}}[\![\mathtt{while}\ ^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!] \tag{8}$$

$$\mathscr{F}^*_{\mathbb{V}}[\![\texttt{while}^{\ell}\ \texttt{(B)}\ \texttt{S}_b]\!]\ X \triangleq \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \tag{8.a}$$

$$\cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{aft}[\![\texttt{S}]\!],\ \rho\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathscr{B}[\![\texttt{B}]\!]\ \rho = \mathtt{ff} \wedge \ell' = \ell\}^{6} \tag{8.b}$$

$$\cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{at}[\![\texttt{S}_b]\!],\ \rho\rangle\pi_3 \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathscr{B}[\![\texttt{B}]\!]\ \rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\texttt{S}_b]\!],\ \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{V}}[\![\texttt{S}_b]\!] \wedge \ell' = \ell\} \tag{8.c}$$

- The other cases are similar.
- Observe than the only difference between real ($\mathbb{V} = \mathbb{R}$) and float ($\mathbb{V} = \mathbb{F}$) computations is the constant $0.1_{\mathbb{V}}$ and the difference $-_{\mathbb{V}}$, which for floats depends on the rounding mode (round-to $+\infty$, round-to $-\infty$, round-to 0, or round-to-nearest). For simplicity, we assume that the rounding mode is fixed, not changed during execution, and correctly taken into account by these operations.

Maximal trace semantics Let $\mathbb{V}$ be $\mathbb{R}$, $\mathbb{F}$, or $\mathbb{I}$. The maximal trace semantics $\mathscr{S}^{+\infty}_{\mathbb{V}}[\![\texttt{S}]\!] = \mathscr{S}^{+}_{\mathbb{V}}[\![\texttt{S}]\!] \cup \mathscr{S}^{\infty}_{\mathbb{V}}[\![\texttt{S}]\!]$ is derived from the prefix trace semantics $\mathscr{S}^*_{\mathbb{V}}[\![\texttt{S}]\!]$ by keeping the longest finite traces $\mathscr{S}^{+}_{\mathbb{V}}[\![\texttt{S}]\!]$ and passing to the limit $\mathscr{S}^{\infty}_{\mathbb{V}}[\![\texttt{S}]\!]$ of prefix-closed traces for infinite traces.

$$\mathscr{S}^{+}_{\mathbb{V}}[\![\texttt{S}]\!] \triangleq \{\pi^{\ell} \in \mathscr{S}^*_{\mathbb{V}}[\![\texttt{S}]\!] \mid (\ell = \mathsf{aft}[\![\texttt{S}]\!]) \vee (\mathsf{esc}[\![\texttt{S}]\!] \wedge \ell = \mathsf{brk\text{-}to}[\![\texttt{S}]\!])\} \tag{9}$$

$$\mathscr{S}^{\infty}_{\mathbb{V}}[\![\texttt{S}]\!] \triangleq \lim(\mathscr{S}^*_{\mathbb{V}}[\![\texttt{S}]\!]) \tag{10}$$

$$\text{where the limit is } \lim \mathcal{T} \triangleq \{\pi \in \mathbb{S}^{\infty}_{\mathbb{V}} \mid \forall n \in \mathbb{N}\ .\ \pi[0..n] \in \mathcal{T}\}. \tag{11}$$

The intuition for (11) is the following. Let $\texttt{S}$ be an iteration. $\pi \in \mathscr{S}^{\infty}_{\mathbb{V}}[\![\texttt{S}]\!] = \lim \mathscr{S}^*_{\mathbb{V}}[\![\texttt{S}]\!]$ where π is infinite if and only if, whenever we take a prefix $\pi[0..n]$ of π, it is a possible finite observation of the execution of $\texttt{S}$ and so belongs to the prefix trace semantics $\pi[0..n] \in \mathscr{S}^*_{\mathbb{V}}[\![\texttt{S}]\!]$.

3 Float intervals

Let $\lfloor x$ (which may be $-\infty$) be the largest float smaller than or equal to $x \in \mathbb{R}$ (or $\lfloor x = x$ for $x \in \mathbb{F}$) and $x\rceil$ (which may be $+\infty$) be the smallest float greater than or equal to $x \in \mathbb{R}$ (or $x\rceil = x$ for $x \in \mathbb{F}$). We let $\lfloor\!\lfloor x$ be the largest floating-point number strictly less than $x \in \mathbb{F}$ (which may be $-\infty$) and $x\rceil\!\rceil$ be the smallest floating-point number strictly larger than $x \in \mathbb{F}$ (which may be $+\infty$). We assume that

$$\lfloor x -_{\mathbb{F}} y\rceil \leqslant \lfloor (x -_{\mathbb{V}} y) \qquad (\mathbb{V} \text{ is } \mathbb{R} \text{ or } \mathbb{F}) \tag{12}$$
$$x\rceil -_{\mathbb{F}} \lfloor y \geqslant (x -_{\mathbb{V}} y)\rceil$$

$$(\mathsf{x} \in [\underline{x}, \overline{x}] \wedge \mathsf{y} \in [\underline{y}, \overline{y}] \wedge \mathsf{x} < \mathsf{y}) \Rightarrow (\mathsf{x} \in [\underline{x}, \min(\overline{x}, \overline{y})] \wedge \mathsf{y} \in [\max(\underline{x}, \underline{y}), \overline{y}]) \tag{13}$$

$$(\mathsf{x} \in [\underline{x}, \overline{x}] \wedge \mathsf{y} \in [\underline{y}, \overline{y}] \wedge \mathsf{x} < \mathsf{y}) \Rightarrow (\mathsf{x} \in [\underline{x}, \min(\overline{x}, \overline{y}\rceil\!\rceil)] \wedge \mathsf{y} \in [\max(\lfloor\!\lfloor \underline{x}, \underline{y}), \overline{y}]) \tag{13.bis}$$

[6] A definition of the form $d(\vec{x}) \triangleq \{f(\vec{x}') \mid P(\vec{x}', \vec{x})\}$ has the variables $\vec{x}'$ in $P(\vec{x}', \vec{x})$ bound to those of $f(\vec{x}')$ whereas $\vec{x}$ is free in $P(\vec{x}', \vec{x})$ since it appears neither in $f(\vec{x}')$ nor (by assumption) under quantifiers in $P(\vec{x}', \vec{x})$. The $\vec{x}$ of $P(\vec{x}', \vec{x})$ is therefore bound to the $\vec{x}$ of $d(\vec{x})$.

Machine implementations of IEEE-754 floating point arithmetics [24] are sometimes incorrect [14,30]. So the above hypotheses (12) and (13) on floats must be adjusted accordingly, for example replacing (13) by (13.bis). In particular (13.bis) follows the recommendation of [30, Sect. 6.1.2]. If $\mathtt{x} < \mathtt{y}$ then the value of $\mathtt{x}$ is smaller than its maximal value $\overline{x}$ and the maximal $\overline{y}$ value of $\mathtt{y}$, by precaution, certainly smaller or equal to the next float greater that $\overline{y}$.

4 Abstraction of real traces by float interval traces

Given a real trace semantics *i.e.* a set $\Pi \in \wp(\mathbb{S}^{+\infty}_{\mathbb{R}})$, we define a float interval trace semantics by abstracting the real $x \in \mathbb{R}$ values by an interval $[\overleftarrow{\P} x, x \overrightarrow{\P}]$. More precisely, since abstract interpretation is about the abstraction of properties, the strongest property $\{x\} \in \wp(\mathbb{R})$ of this value is over-approximated by a weaker interval property, that is $\{x\} \subseteq [\overleftarrow{\P} x, x \overrightarrow{\P}]$, or equivalently $x \in [\overleftarrow{\P} x, x \overrightarrow{\P}]$. Formally

$$
\begin{array}{rcll}
\alpha^{\mathbb{I}}(x) & \triangleq & [\overleftarrow{\P} x, x \overrightarrow{\P}] & \text{real abstraction by float interval} \quad (14)\\
\gamma^{\mathbb{I}}([\underline{x}, \overline{x}]) & \triangleq & \{x \in \mathbb{R} \mid \underline{x} \leqslant x \leqslant \overline{x}\} & \\
\dot{\alpha}^{\mathbb{I}}(\rho) & \triangleq & \lambda\, \mathtt{x} \in \mathbb{X} \bullet \alpha^{\mathbb{I}}(\rho(\mathtt{x})) & \text{environment abstraction}\\
\dot{\gamma}^{\mathbb{I}}(\overline{\rho}) & \triangleq & \{\rho \in \mathbb{X} \to \mathbb{R} \mid \forall \mathtt{x} \in \mathbb{X} \,.\, \rho(\mathtt{x}) \in \gamma^{\mathbb{I}}(\overline{\rho}(\mathtt{x}))\} & \\
\ddot{\alpha}^{\mathbb{I}}(\langle \ell,\, \rho \rangle) & \triangleq & \langle \ell,\, \dot{\alpha}^{\mathbb{I}}(\rho) \rangle & \text{state abstraction}\\
\ddot{\gamma}^{\mathbb{I}}(\langle \ell,\, \overline{\rho} \rangle) & \triangleq & \{\langle \ell,\, \rho \rangle \mid \rho \in \dot{\gamma}^{\mathbb{I}}(\overline{\rho})\} & \\
\vec{\alpha}^{\mathbb{I}}(\pi_1 \ldots \pi_n \ldots) & \triangleq & \ddot{\alpha}^{\mathbb{I}}(\pi_1) \ldots \ddot{\alpha}^{\mathbb{I}}(\pi_n) \ldots & \text{[in]finite trace abstraction}\\
\vec{\gamma}^{\mathbb{I}}(\overline{\pi}_1 \ldots \overline{\pi}_n \ldots) & \triangleq & \{\pi_1 \ldots \pi_n \ldots \mid |\pi| = |\overline{\pi}| \wedge \forall i = 1, \ldots, n, \ldots \,.\, \pi_i \in \ddot{\gamma}^{\mathbb{I}}(\overline{\pi}_i)\} & \\
\mathring{\alpha}^{\mathbb{I}}(\Pi) & \triangleq & \{\vec{\alpha}^{\mathbb{I}}(\pi) \mid \pi \in \Pi\} & \text{set of traces abstraction}\\
\mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}) & \triangleq & \{\pi \mid \vec{\alpha}^{\mathbb{I}}(\pi) \in \overline{\Pi}\} = \bigcup \{\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \mid \overline{\pi} \in \overline{\Pi}\} &
\end{array}
$$

Because the floats are a subset of the reals, we can use $\alpha^{\mathbb{I}}$ to abstract both real and float traces in (14) (*i.e.* $\mathbb{R}$ becomes $\mathbb{V}$ standing for $\mathbb{R}$ or $\mathbb{F}$).

$$
\langle \wp(\mathbb{S}^{+\infty}_{\mathbb{V}}),\, \subseteq \rangle \underset{\mathring{\alpha}^{\mathbb{I}}}{\overset{\mathring{\gamma}^{\mathbb{I}}}{\leftrightarrows}} \langle \wp(\mathbb{S}^{+\infty}_{\mathbb{I}}),\, \subseteq \rangle \tag{15}
$$

Proof (of (15)).

$$
\begin{array}{ll}
\quad \mathring{\alpha}^{\mathbb{I}}(\Pi) \subseteq \overline{\Pi} & \\
\Leftrightarrow \{\vec{\alpha}^{\mathbb{I}}(\pi) \mid \pi \in \Pi\} \subseteq \overline{\Pi} & \wr \text{def. (14) of } \mathring{\alpha}^{\mathbb{I}} \int \\
\Leftrightarrow \forall \pi \in \Pi \,.\, \vec{\alpha}^{\mathbb{I}}(\pi) \in \overline{\Pi} & \wr \text{def. } \subseteq \int \\
\Leftrightarrow \Pi \subseteq \{\pi \mid \vec{\alpha}^{\mathbb{I}}(\pi) \in \overline{\Pi}\} & \wr \text{def. } \subseteq \int \\
\Leftrightarrow \Pi \subseteq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}) & \wr \text{by defining } \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}) \triangleq \{\pi \mid \vec{\alpha}^{\mathbb{I}}(\pi) \in \overline{\Pi}\} \int
\end{array}
$$

where

$$
\begin{array}{ll}
\quad \vec{\alpha}^{\mathbb{I}}(\pi) \in \overline{\Pi} & \\
\Leftrightarrow \exists \overline{\pi} \in \overline{\Pi} \,.\, \vec{\alpha}^{\mathbb{I}}(\pi) = \overline{\pi} & \wr \text{def. } \in \int
\end{array}
$$

$\Leftrightarrow \exists \overline{\pi} \in \overline{\Pi} \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi})$ ⟅def. $\vec{\alpha}^{\mathbb{I}}(\pi)$ and $\vec{\gamma}^{\mathbb{I}}(\overline{\pi})$⟆

$\Leftrightarrow \pi \in \bigcup_{\overline{\pi} \in \overline{\Pi}} \vec{\gamma}^{\mathbb{I}}(\overline{\pi})$ ⟅def. $\cup$⟆

and therefore

$\mathring{\gamma}^{\mathbb{I}}(\overline{\Pi})$

$\triangleq \{\pi \mid \vec{\alpha}^{\mathbb{I}}(\pi) \in \overline{\Pi}\}$ ⟅def. $\gamma^{\mathbb{I}}$⟆

$= \{\pi \mid \pi \in \bigcup_{\overline{\pi} \in \overline{\Pi}} \vec{\gamma}^{\mathbb{I}}(\overline{\pi})\} = \bigcup \{\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \mid \overline{\pi} \in \overline{\Pi}\}$ ⟅as shown above⟆ □

5 Sound over-approximation in the concrete

Let $\Pi = \{\langle \ell_1,\ \mathtt{x} = 0.1_{\mathbb{R}} \rangle \langle \ell_2,\ \mathtt{x} = 2.1_{\mathbb{R}} \rangle, \langle \ell_1,\ \mathtt{x} = -0.1_{\mathbb{R}} \rangle \langle \ell_2,\ \mathtt{x} = 1.9_{\mathbb{R}} \rangle\}$. Assume that $\overline{\Pi}_1 = \alpha^{\mathbb{I}}(\Pi) = \{\langle \ell_1,\ \mathtt{x} = [0.09, 0.11] \rangle \langle \ell_2,\ \mathtt{x} = [2.09, 2.11] \rangle, \langle \ell_1,\ \mathtt{x} = [-0.11, -0.09] \rangle \langle \ell_2,\ \mathtt{x} = [1.89, 1.91] \rangle\}$ where each trace π of Π is over-approximated by a trace $\vec{\alpha}^{\mathbb{I}}(\pi)$ of $\overline{\Pi}_1$ with a ± 0.01 rounding interval. We have $\Pi \subseteq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}_1)$ so $\overline{\Pi}_1$ is a sound over-approximation of Π. But $\overline{\Pi}_2 = \{\langle \ell_1,\ \mathtt{x} = [-0.11, 0.11] \rangle \langle \ell_2,\ \mathtt{x} = [1.89, 2.11] \rangle\}$ is also a sound over-approximation of Π since $\Pi \subseteq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}_2)$. Although $\overline{\Pi}_1 \in \wp(\mathbb{S}^{+\infty}_{\mathbb{I}})$ is more precise than $\overline{\Pi}_2 \in \wp(\mathbb{S}^{+\infty}_{\mathbb{I}})$, they are not comparable as abstract elements of $\langle \wp(\mathbb{S}^{+\infty}_{\mathbb{I}}), \subseteq \rangle$ in (15). The intuition that $\overline{\Pi}_1$ is more precise than $\overline{\Pi}_2$ is by comparison in the concrete that is $\mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}_1) \subseteq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}_2)$. We now express this preorder relation $\mathring{\sqsubseteq}^{i}$ between $\overline{\Pi}_1$ and $\overline{\Pi}_2$ which will allow us to over-approximate intervals when needed.

$$\begin{aligned} \overline{\Pi} \,\mathring{\sqsubseteq}^{i}\, \overline{\Pi}' &\triangleq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}) \subseteq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}') \\ &= \forall \overline{\pi} \in \overline{\Pi} \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \,.\, \exists \overline{\pi}' \in \overline{\Pi}' \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}') \end{aligned} \tag{16}$$

Proof (of (16)).

$\overline{\Pi} \,\mathring{\sqsubseteq}^{i}\, \overline{\Pi}'$

$\triangleq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}) \subseteq \mathring{\gamma}^{\mathbb{I}}(\overline{\Pi}')$ ⟅(16)⟆

$= \bigcup \{\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \mid \overline{\pi} \in \overline{\Pi}\} \subseteq \bigcup \{\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \mid \overline{\pi} \in \overline{\Pi}'\}$ ⟅(14) for sets of traces⟆

$= \forall \overline{\pi} \in \overline{\Pi} \,.\, \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \subseteq \bigcup \{\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \mid \overline{\pi} \in \overline{\Pi}'\}$ ⟅def. $\subseteq$⟆

$= \forall \overline{\pi} \in \overline{\Pi} \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \,.\, \pi \in \bigcup \{\vec{\gamma}^{\mathbb{I}}(\overline{\pi}') \mid \overline{\pi}' \in \overline{\Pi}'\}$ ⟅def. $\subseteq$⟆

$= \forall \overline{\pi} \in \overline{\Pi} \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \,.\, \exists \overline{\pi}' \in \overline{\Pi}' \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$ ⟅def. $\bigcup$⟆ □

It follows that we have a Galois connection (note that the abstract preorder and concretization are different from (15))

$$\langle \wp(\mathbb{S}^{+\infty}_{\mathbb{V}}), \subseteq \rangle \underset{\mathring{\alpha}^{\mathbb{I}}}{\overset{\mathring{\vec{\gamma}}}{\leftrightarrows}} \langle \wp(\mathbb{S}^{+\infty}_{\mathbb{I}}), \mathring{\sqsubseteq}^{i} \rangle \tag{17}$$

Proof (of (17)).

$\mathring{\alpha}^{\mathbb{I}}(\Pi) \,\mathring{\sqsubseteq}^{i}\, \overline{\Pi}$

$\Leftrightarrow \{\vec{\alpha}^{\mathbb{I}}(\pi) \mid \pi \in \Pi\} \,\mathring{\sqsubseteq}^{i}\, \overline{\Pi}$ ⟅def. (14) of $\mathring{\alpha}^{\mathbb{I}}$⟆

$\Leftrightarrow \forall \overline{\pi} \in \{\vec{\alpha}^{\mathbb{I}}(\pi') \mid \pi' \in \Pi\} \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \,.\, \exists \overline{\pi}' \in \overline{\Pi} \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$ ⟅def. (16) of $\mathring{\sqsubseteq}^i$⟆

$\Leftrightarrow \forall \pi' \in \Pi \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\vec{\alpha}^{\mathbb{I}}(\pi')) \,.\, \exists \overline{\pi}' \in \overline{\Pi} \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$ ⟅def. ∈⟆

$\Leftrightarrow \Pi \subseteq \{\pi' \mid \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\vec{\alpha}^{\mathbb{I}}(\pi')) \,.\, \exists \overline{\pi}' \in \overline{\Pi} \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')\}$ ⟅def. ⊆⟆

$\Leftrightarrow \Pi \subseteq \mathring{\gamma}(\overline{\Pi})$

by defining $\mathring{\gamma}(\overline{\Pi}) \triangleq \{\pi' \mid \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\vec{\alpha}^{\mathbb{I}}(\pi')) \,.\, \exists \overline{\pi}' \in \overline{\Pi} \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')\}$. □

Soundness is now $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{s}]\!]) \mathrel{\mathring{\sqsubseteq}^i} \boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathsf{s}]\!]$ or equivalently $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{s}]\!] \subseteq \mathring{\gamma}(\boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathsf{s}]\!])$. Our objective is to calculate $\boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathsf{s}]\!]$ by $\mathring{\sqsubseteq}^i$-over approximation of $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{s}]\!])$. However $\mathring{\sqsubseteq}^i$ in (16) is impractical since it is defined by concretization to $\wp(\mathbb{S}^{+\infty}_{\mathbb{V}})$. We look for a definition $\mathring{\sqsubseteq}^i$ in the abstract only that provides a sufficient soundness condition $(\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}') \Rightarrow (\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}')$.

6 Sound over-approximation in the abstract

We define $\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}'$ so that the traces of $\overline{\Pi}'$ have the same control as the traces of $\overline{\Pi}$ but intervals are larger (and $\overline{\Pi}'$ may contain extra traces due to the imprecision of interval tests).

Formally, the interval order $\sqsubseteq^i$ is extended pointwise $\dot{\sqsubseteq}^i$ to environments, and to states $\ddot{\sqsubseteq}^i$ with same control points/program labels. Then it is extended $\vec{\sqsubseteq}^i$ to traces of same length with same control but larger intervals, and finally to sets of traces, by Hoare preorder [41].

$$
\begin{aligned}
[\underline{x}, \overline{x}] \sqsubseteq^i [\underline{y}, \overline{y}] &\triangleq \underline{y} \leqslant \underline{x} \leqslant \overline{x} \leqslant \overline{y} \\
\rho \mathrel{\dot{\sqsubseteq}^i} \rho' &\triangleq \forall \mathsf{x} \in \mathbb{X} \,.\, \rho(\mathsf{x}) \sqsubseteq^i \rho'(\mathsf{x}) \\
\langle \ell, \rho \rangle \mathrel{\ddot{\sqsubseteq}^i} \langle \ell', \rho' \rangle &\triangleq (\ell = \ell') \wedge (\rho \mathrel{\dot{\sqsubseteq}^i} \rho') \\
\overline{\pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}' &\triangleq (|\overline{\pi}| = |\overline{\pi}'|) \wedge (\forall i \in [0, |\overline{\pi}|[\,.\, \overline{\pi}_i \mathrel{\ddot{\sqsubseteq}^i} \overline{\pi}'_i) \\
\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}' &\triangleq \forall \overline{\pi} \in \overline{\Pi} \,.\, \exists \overline{\pi}' \in \overline{\Pi}' \,.\, \overline{\pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}'
\end{aligned}
\tag{18}
$$

Lemma 1. $(\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}') \Rightarrow (\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}')$. □

Proof (of Lem. 1). By (14) and (18), we have $[\underline{x}, \overline{x}] \sqsubseteq^i [\underline{y}, \overline{y}]$ implies $\gamma^{\mathbb{I}}([\underline{x}, \overline{x}]) \subseteq \gamma^{\mathbb{I}}([\underline{y}, \overline{y}])$ and so $\rho \mathrel{\dot{\sqsubseteq}^i} \rho'$ implies $\gamma^{\mathbb{I}}(\rho) \subseteq \dot{\gamma}^{\mathbb{I}}(\rho')$ and therefore $\langle \ell, \rho \rangle \mathrel{\ddot{\sqsubseteq}^i} \langle \ell', \rho' \rangle$ implies $\gamma^{\mathbb{I}}(\langle \ell, \rho \rangle) \subseteq \gamma^{\mathbb{I}}(\langle \ell', \rho' \rangle)$ so that finally $\overline{\pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}'$ implies $\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \subseteq \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$. It follows that

$\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}'$

$\Leftrightarrow \forall \overline{\pi} \in \overline{\Pi} \,.\, \exists \overline{\pi}' \in \overline{\Pi}' \,.\, \overline{\pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}'$ ⟅def. (18) of $\mathring{\sqsubseteq}^i$⟆

$\Rightarrow \forall \overline{\pi} \in \overline{\Pi} \,.\, \exists \overline{\pi}' \in \overline{\Pi}' \,.\, \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \subseteq \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$ ⟅since $\overline{\pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}'$ implies $\vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \subseteq \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$⟆

$\Rightarrow \forall \overline{\pi} \in \overline{\Pi} \,.\, \exists \overline{\pi}' \in \overline{\Pi}' \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}')$ ⟅def. ⊆⟆

$\Rightarrow \forall \overline{\pi} \in \overline{\Pi} \,.\, \forall \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}) \,.\, \exists \overline{\pi}'' \in \overline{\Pi}' \,.\, \pi \in \vec{\gamma}^{\mathbb{I}}(\overline{\pi}'')$
$\qquad\qquad$ ⟅choosing the same $\overline{\pi}'' = \overline{\pi}'$ for all π⟆
$\Leftrightarrow \overline{\Pi} \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \overline{\Pi}'$ ⟅(16)⟆ □

It follows that we have a Galois connection (note that the abstract preorder and concretization are different from both (15) and (17))

$$\langle \wp(\mathbb{S}^{+\infty}_{\mathbb{V}}), \subseteq \rangle \underset{\mathring{\alpha}^{\mathbb{I}}}{\overset{\mathring{\vec{\gamma}}}{\leftrightarrows}} \langle \wp(\mathbb{S}^{+\infty}_{\mathbb{I}}), \mathring{\vec{\sqsubseteq}}^{i} \rangle \tag{19}$$

Proof (of (19)).

$\mathring{\alpha}^{\mathbb{I}}(\Pi) \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \overline{\Pi}$
$\Leftrightarrow \{\vec{\alpha}^{\mathbb{I}}(\pi) \mid \pi \in \Pi\} \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \overline{\Pi}$ ⟅def. (14) of $\mathring{\alpha}^{\mathbb{I}}$⟆
$\Leftrightarrow \forall \overline{\pi} \in \{\vec{\alpha}^{\mathbb{I}}(\pi) \mid \pi \in \Pi\} \,.\, \exists \overline{\pi}' \in \overline{\Pi} \,.\, \overline{\pi} \mathrel{\vec{\sqsubseteq}^{i}} \overline{\pi}'$ ⟅def. (18) of $\mathring{\vec{\sqsubseteq}}^{i}$⟆
$\Leftrightarrow \forall \pi \in \Pi \,.\, \exists \overline{\pi}' \in \overline{\Pi} \,.\, \vec{\alpha}^{\mathbb{I}}(\pi) \mathrel{\vec{\sqsubseteq}^{i}} \overline{\pi}'$ ⟅def. $\in$⟆
$\Leftrightarrow \Pi \subseteq \{\pi \mid \exists \overline{\pi}' \in \overline{\Pi} \,.\, \vec{\alpha}^{\mathbb{I}}(\pi) \mathrel{\vec{\sqsubseteq}^{i}} \overline{\pi}'\}$ ⟅def. $\subseteq$⟆
$\Leftrightarrow \Pi \subseteq \mathring{\vec{\gamma}}(\overline{\Pi})$
by defining $\mathring{\vec{\gamma}}(\overline{\Pi}) \triangleq \{\pi \mid \exists \overline{\pi}' \in \overline{\Pi} \,.\, \vec{\alpha}^{\mathbb{I}}(\pi) \mathrel{\vec{\sqsubseteq}^{i}} \overline{\pi}'\}$. □

7 Calculational design of the float interval trace semantics

The float interval trace semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$ of a program component $\mathtt{s}$ replaces concrete real or float traces (as defined by $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]$) by interval traces. It is sound if and only if the concrete traces are included in the abstract traces that is $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!] \subseteq \mathring{\gamma}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!])$ or, equivalently, by (15), $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]) \subseteq \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$.

Although, the soundness condition $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]) \subseteq \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$ allows the abstract semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$ to contain more traces, including with larger intervals, it requires the abstract traces in $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!])$ (which are the best float interval abstractions of real computations) to all belong to the abstract semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$.

We introduced $\mathring{\vec{\sqsubseteq}}^{i}$ in (18) to relax this requirement about the presence of best interval trace abstractions of real computations in the abstract semantics. The weaker requirement $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!])$ implies, by Lem. 1, that $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!])$ so that, by (16), $\mathring{\gamma}^{\mathbb{I}}(\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!])) \subseteq \mathring{\gamma}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!])$, which, together with $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!] \subseteq \mathring{\gamma}^{\mathbb{I}}(\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]))$ from the Galois connection (15) yields, by transitivity, that $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!] \subseteq \mathring{\gamma}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!])$.

This weaker soundness requirement $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!])$ yields a calculational design method where $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!])$ is $\mathring{\vec{\sqsubseteq}}^{i}$-over-approximated so as to eliminate any reference to the concrete semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]$. We proceed by structural induction on $\lhd$, assuming $\mathring{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{s}']\!]) \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}']\!]$ for all $\mathtt{s}' \lhd \mathtt{s}$.

To design $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$ such that $\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{S}}_{\mathbb{R}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\vec{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{I}}[\![\mathtt{s}]\!]$ by structural induction, we will need to prove a stronger result stating that any interval overapproximation of an initial state of a real computation can be extended into an interval computation abstracting this real computation. Formally, we have

$$\forall \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\pi \in X\ .\ \forall \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\ . \qquad (20)$$
$$(\dot{\alpha}^{\mathbb{I}}(\rho) \mathrel{\dot{\sqsubseteq}^i} \overline{\rho}) \Rightarrow (\exists \overline{\pi}\ .\ \alpha^{\mathbb{I}}(\pi) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi} \wedge \langle \mathsf{at}[\![\mathtt{S}]\!],\ \overline{\rho}\rangle\overline{\pi} \in \overline{X})$$

which we will use for $X = \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ and $\overline{X} = \boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathtt{S}]\!]$ is well as for the concrete X and abstract $\overline{X}$ fixpoint iterates in (8) for iteration statements.

Interval abstraction of an arithmetic expression Given $\rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}$ (where $\mathbb{V}$ is $\mathbb{R}$ or $\mathbb{F}$), let us evaluate $\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho)$ by structural induction on $\mathtt{A}$ and define $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}]\!]$ such that

$$\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho) \mathrel{\dot{\sqsubseteq}^i} \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}]\!]\dot{\alpha}^{\mathbb{I}}(\rho). \qquad (21)$$

— $\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{0.1}]\!]\rho)$
= $\alpha^{\mathbb{I}}(0.1_{\mathbb{V}})$ ⟅def. $\boldsymbol{\mathcal{A}}_{\mathbb{V}}$ in (1)⟆
= $[\overleftarrow{\P}0.1_{\mathbb{V}}, 0.1_{\mathbb{V}}\overrightarrow{\P}]$ ⟅real abstraction by float interval in (14)⟆
≜ $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{0.1}]\!](\dot{\alpha}^{\mathbb{I}}(\rho))$ ⟅by defining $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{0.1}]\!]\overline{\rho} \triangleq [\overleftarrow{\P}0.1_{\mathbb{V}}, 0.1_{\mathbb{V}}\overrightarrow{\P}]$⟆

— $\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{x}]\!]\rho)$
= $\alpha^{\mathbb{I}}(\rho(\mathtt{x}))$ ⟅def. $\boldsymbol{\mathcal{A}}_{\mathbb{V}}$ in (1)⟆
= $\dot{\alpha}^{\mathbb{I}}(\rho)(\mathtt{x})$ ⟅def. environment abstraction in (14)⟆
≜ $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{x}]\!](\dot{\alpha}^{\mathbb{I}}(\rho))$ ⟅by defining $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{x}]\!]\overline{\rho} \triangleq \overline{\rho}(\mathtt{x})$⟆

— $\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\rho)$
= $\alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho -_{\mathbb{V}} \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho)$ ⟅def. $\boldsymbol{\mathcal{A}}_{\mathbb{V}}$ in (1)⟆
= $[\overleftarrow{\P}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho -_{\mathbb{V}} \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho), (\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho -_{\mathbb{V}} \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho)\overrightarrow{\P}]$
⟅value abstraction by float interval in (14)⟆
$\mathrel{\dot{\sqsubseteq}^i}$ $[\overleftarrow{\P}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho) -_{\mathbb{F}} (\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho)\overrightarrow{\P}), (\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho)\overrightarrow{\P} -_{\mathbb{F}} \overleftarrow{\P}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho)]$
⟅(18) and hyp. (12)⟆
$\mathrel{\dot{\sqsubseteq}^i}$ $\mathsf{let}\ [\underline{x}, \overline{x}] = \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_1]\!]\dot{\alpha}^{\mathbb{I}}(\rho)\ \mathsf{and}\ [\underline{y}, \overline{y}] = \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_2]\!]\dot{\alpha}^{\mathbb{I}}(\rho)\ \mathsf{in}\ [\underline{x} -_{\mathbb{F}} \overline{y}, \overline{x} -_{\mathbb{F}} \underline{y}]$
⟅By ind. hyp. $[\overleftarrow{\P}\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_i]\!]\rho, \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_i]\!]\rho\overrightarrow{\P}] = \alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}_i]\!]\rho) \mathrel{\dot{\sqsubseteq}^i} \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_i]\!]\dot{\alpha}^{\mathbb{I}}(\rho)$, $i = 1, 2$.⟆
= $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_1]\!]\dot{\alpha}^{\mathbb{I}}(\rho) -_{\mathbb{I}} \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_2]\!]\dot{\alpha}^{\mathbb{I}}(\rho)$ ⟅by defining $[\underline{x}, \overline{x}] -_{\mathbb{I}} [\underline{y}, \overline{y}] \triangleq [\underline{x} -_{\mathbb{F}} \overline{y}, \overline{x} -_{\mathbb{F}} \underline{y}]$⟆
≜ $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\dot{\alpha}^{\mathbb{I}}(\rho)$ ⟅by defining $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\overline{\rho} \triangleq \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_1]\!]\overline{\rho} -_{\mathbb{I}} \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}_2]\!]\overline{\rho}$⟆

We observe that $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}]\!]$ is $\mathrel{\dot{\sqsubseteq}^i}$-increasing. □

If we had a division, we would have to handle NaN. A simple way is to stop execution, by choosing $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{1/0}]\!]\overline{\rho} \triangleq \varnothing$. Another way would be to include the NaN in the abstraction by considering $\mathsf{N}[\underline{x}, \overline{x}]$ meaning a float between the bounds while $\mathsf{NaN}[\underline{x}, \overline{x}]$ would mean a float between the bounds or NaN. We chose the first alternative, which is simpler.

Interval trace semantics of an assignment statement We can now abstract the semantics of real ($\mathbb{V} = \mathbb{R}$) or float ($\mathbb{V} = \mathbb{F}$) assignments by float intervals.

$$
\begin{array}{ll}
& \dot{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]) \qquad \text{〈where } \mathtt{S} = \ell\ \mathtt{x = A\ ;}\text{〉} \\
= & \{\alpha^{\mathbb{I}}(\pi) \mid \pi \in \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\ell\ \mathtt{x = A\ ;}]\!]\} \qquad \text{〈set of traces abstraction (14)〉} \\
= & \{\alpha^{\mathbb{I}}(\pi) \mid \pi \in \{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \cup \{\langle \ell, \rho\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \rho[\mathtt{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\}\} \\
& \qquad \text{〈def. } \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\ell\ \mathtt{x = A\ ;}]\!] \text{ in (2)〉} \\
= & \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \cup \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \alpha^{\mathbb{I}}(\rho[\mathtt{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho])\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \\
& \qquad \text{〈def. (14) of trace abstraction〉} \\
= & \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \cup \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \dot{\alpha}^{\mathbb{I}}(\rho)[\mathtt{x} \leftarrow \alpha^{\mathbb{I}}(\boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho])\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \\
& \qquad \text{〈def. (14) of environment abstraction〉} \\
\dot{\sqsubseteq}^i & \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \cup \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \dot{\alpha}^{\mathbb{I}}(\rho)[\mathtt{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}]\!]\dot{\alpha}^{\mathbb{I}}(\rho)]\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \\
& \qquad \text{〈def. (18) of } \dot{\sqsubseteq}^i \text{ and (21)〉} \\
\dot{\sqsubseteq}^i & \{\langle \ell, \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\} \cup \{\langle \ell, \overline{\rho}\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \overline{\rho}[\mathtt{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}]\!]\overline{\rho}]\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\} \\
& \qquad \text{〈}\{\dot{\alpha}^{\mathbb{I}}(\rho) \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \subseteq \mathbb{E}\mathbb{v}_{\mathbb{I}} \text{ by (14) for environment abstraction〉} \\
\triangleq & \ \boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\ell\ \mathtt{x = A\ ;}]\!] \qquad \text{〈by defining } \boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\ell\ \mathtt{x = A\ ;}]\!] \text{ as in (2) for } \mathbb{V} = \mathbb{I}\text{〉}
\end{array}
$$

(20) follows from $\boldsymbol{\mathcal{A}}_{\mathbb{I}}[\![\mathtt{A}]\!]$ is $\dot{\sqsubseteq}^i$-increasing. □

Interval trace semantics of a break statement

$$
\begin{array}{ll}
& \dot{\alpha}^{\mathbb{I}}(\boldsymbol{\mathcal{S}}^*_{\mathbb{R}}[\![\mathtt{S}]\!]) \qquad \text{〈where } \mathtt{S} = \ell\ \mathtt{break\ ;}\text{〉} \\
\triangleq & \ \dot{\alpha}^{\mathbb{I}}(\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \cup \{\langle \ell, \rho\rangle\langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!], \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{R}}\}) \qquad \text{〈(3)〉} \\
= & \ \dot{\alpha}^{\mathbb{I}}(\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{R}}\}) \cup \alpha^{\mathbb{I}}(\{\langle \ell, \rho\rangle\langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!], \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{R}}\}) \\
& \qquad \text{〈the abstraction preserves joins in the Galois connection (15)〉} \\
= & \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{R}}\} \cup \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!], \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{R}}\} \\
& \qquad \text{〈def. (14) of } \dot{\alpha}^{\mathbb{I}} \text{〉} \\
\dot{\sqsubseteq}^i & \{\langle \ell, \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\} \cup \{\langle \ell, \overline{\rho}\rangle\langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!], \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\} \qquad \text{〈}\{\dot{\alpha}^{\mathbb{I}}(\rho) \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \subseteq \mathbb{E}\mathbb{v}_{\mathbb{I}}\text{〉} \\
\triangleq & \ \boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathtt{S}]\!] \qquad \text{〈by defining } \boldsymbol{\mathcal{S}}^*_{\mathbb{I}}[\![\mathtt{S}]\!] \text{ as in (3) for } \mathbb{V} = \mathbb{I}\text{〉}
\end{array}
$$

(20) follows from $\overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}$ and $\overline{\rho} \dot{\sqsubseteq}^i \overline{\rho}'$ implies $\overline{\rho}' \in \mathbb{E}\mathbb{v}_{\mathbb{I}}$. □

Interval trace semantics of the statement list Given sets of traces $\Pi_1, \Pi_2 \in \wp(\mathbb{S}^*_{\mathbb{V}})$, let us calculate

$$
\begin{array}{ll}
& \alpha^{\mathbb{I}}(\Pi_1 \mathbin{\hat{\cdot}} \Pi_2) \\
= & \alpha^{\mathbb{I}}(\{\pi_1\sigma\pi_2 \mid \pi_1\sigma \in \Pi_1 \wedge \sigma\pi_2 \in \Pi_2\}) \qquad \text{〈def. } \hat{\cdot}\text{〉} \\
= & \{\alpha^{\mathbb{I}}(\pi_1\sigma\pi_2) \mid \pi_1\sigma \in \Pi_1 \wedge \sigma\pi_2 \in \Pi_2\} \qquad \text{〈def. } \alpha^{\mathbb{I}}\text{〉} \\
= & \{\alpha^{\mathbb{I}}(\pi_1\sigma) \mathbin{\hat{\cdot}} \alpha^{\mathbb{I}}(\sigma\pi_2) \mid \pi_1\sigma \in \Pi_1 \wedge \sigma\pi_2 \in \Pi_2\} \qquad \text{〈def. } \hat{\cdot}\text{〉} \\
= & \{\overline{\pi_1\,\sigma} \mathbin{\hat{\cdot}} \overline{\sigma\,\pi_2} \mid \overline{\pi_1\,\sigma} \in \alpha^{\mathbb{I}}(\Pi_1) \wedge \overline{\sigma\pi_2} \in \alpha^{\mathbb{I}}(\Pi_2)\} \\
& \qquad \text{〈letting } \overline{\pi_1\sigma} = \alpha^{\mathbb{I}}(\pi_1\sigma) \text{ and } \overline{\sigma\,\pi_2} = \alpha^{\mathbb{I}}(\sigma\pi_2)\text{〉}
\end{array}
$$

$$= \alpha^{\mathbb{I}}(\Pi_1) \frown \alpha^{\mathbb{I}}(\Pi_2) \qquad \wr \text{def. } \frown \wr$$

The case of an empty statement list $\mathtt{Sl} ::= \epsilon$ is trivial and we get $\mathcal{S}^*_{\mathbb{I}}[\![\mathtt{Sl}]\!] \triangleq \{\langle \mathsf{at}[\![\mathtt{Sl}]\!], \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathtt{v}_{\mathbb{I}}\}$. For a non-empty statement list $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$, we have

$$\begin{aligned}
&\dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}]\!]) \\
\triangleq\ &\dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}']\!] \cup \mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}']\!] \frown \mathcal{S}^*_{\mathbb{R}}[\![\mathtt{S}]\!]) && \wr (7) \wr \\
=\ &\dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}']\!]) \cup \dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}']\!] \frown \mathcal{S}^*_{\mathbb{R}}[\![\mathtt{S}]\!]) \\
& && \wr \text{the abstraction preserves joins in the Galois connection (15)} \wr \\
=\ &\dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}']\!]) \cup \dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{Sl}']\!]) \frown \dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{S}]\!]) && \wr \text{as shown above} \wr \\
\dot{\sqsubseteq}^i\ &\mathcal{S}^*_{\mathbb{I}}[\![\mathtt{Sl}']\!] \cup \mathcal{S}^*_{\mathbb{I}}[\![\mathtt{Sl}']\!] \frown \mathcal{S}^*_{\mathbb{I}}[\![\mathtt{S}]\!] \\
& \wr \text{hyp. ind., } (\overline{\Pi}_0 \dot{\sqsubseteq}^i \overline{\Pi}'_0 \wedge \overline{\Pi}_1 \dot{\sqsubseteq}^i \overline{\Pi}'_1) \text{ implies } (\overline{\Pi}_0 \frown \overline{\Pi}_1 \dot{\sqsubseteq}^i \overline{\Pi}'_0 \frown \overline{\Pi}'_1) \text{ and} \\
& (\overline{\Pi}_0 \cup \overline{\Pi}_1 \dot{\sqsubseteq}^i \overline{\Pi}'_0 \cup \overline{\Pi}'_1) \wr
\end{aligned}$$

(20) follows by ind. hyp. and def. $\frown$. □

Interval abstraction of a boolean expression The situation is more complicated for conditionals. While a test is true or false for $\mathbb{V} = \mathbb{R}$ and $\mathbb{V} = \mathbb{F}$, it might be true for part of a float interval and false for another part of this interval when $\mathbb{V} = \mathbb{I}$. Moreover in case of uncertainty (*e.g.* $<$ is handled as $\leqslant$) the two part may overlap.

Therefore we assume that the abstract interpretation $\mathcal{B}_{\mathbb{I}}[\![\mathtt{B}]\!]$ of a boolean expression $\mathtt{B}$ is defined such that

$$\begin{aligned}
&\mathsf{let}\ \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle = \mathcal{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\dot{\alpha}^{\mathbb{I}}(\rho)\ \mathsf{in} && (22)\\
&\quad \dot{\alpha}^{\mathbb{I}}(\rho) \dot{\sqsubseteq}^i \overline{\rho}_{\mathtt{tt}} && \text{if } \mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}\\
&\quad \dot{\alpha}^{\mathbb{I}}(\rho) \dot{\sqsubseteq}^i \overline{\rho}_{\mathtt{ff}} && \text{if } \mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{ff}\\
&\mathsf{and}\ (\langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle = \mathcal{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho}) \Rightarrow (\overline{\rho}_{\mathtt{tt}} \dot{\sqsubseteq}^i \overline{\rho} \wedge \overline{\rho}_{\mathtt{ff}} \dot{\sqsubseteq}^i \overline{\rho})
\end{aligned}$$

stating that no concrete state passing the test is omitted in the abstract and that the postcondition $\overline{\rho}_{\mathtt{tt}}$ or $\overline{\rho}_{\mathtt{ff}}$ is stronger than the precondition $\overline{\rho}$ since, in absence of side effects, the test cannot introduce any new state. Examples of def. of $\mathcal{B}_{\mathbb{V}}$ are found *e.g.* in [3]. If $\mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}$ (respectively $\mathtt{ff}$), there is no constraint on $\overline{\rho}_{\mathtt{ff}}$ (respectively $\overline{\rho}_{\mathtt{tt}}$), the best choice being the $\dot{\sqsubseteq}^i$-infimum empty interval environment $\dot{\varnothing}$.

Interval trace semantics of a conditional statement We can now abstract the semantics of real tests using float intervals.

$$\begin{aligned}
&\dot{\alpha}^{\mathbb{I}}(\mathcal{S}^*_{\mathbb{R}}[\![\mathtt{if}^{\,\ell}\ \mathtt{(B)}\ \mathtt{S}_t]\!]) \\
\triangleq\ &\dot{\alpha}^{\mathbb{I}}(\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathtt{v}_{\mathbb{R}}\} \cup \{\langle \ell, \rho\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \rho\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{ff}\} \cup \{\langle \ell, \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \rho\rangle\pi \mid \\
&\mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_t]\!], \rho\rangle\pi \in \mathcal{S}^*_{\mathbb{R}}[\![\mathtt{S}_t]\!]\}) && \wr \text{def. } \mathcal{S}^*_{\mathbb{R}}[\![\mathtt{if}^{\,\ell}\ \mathtt{(B)}\ \mathtt{S}_t]\!] \text{ in (5)} \wr \\
=\ &\{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \rho \in \mathbb{E}\mathtt{v}_{\mathbb{R}}\} \cup \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{ff}\} \cup \{\langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \\
&\dot{\alpha}^{\mathbb{I}}(\rho)\rangle\alpha^{\mathbb{I}}(\pi) \mid \mathcal{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_t]\!], \rho\rangle\pi \in \mathcal{S}^*_{\mathbb{R}}[\![\mathtt{S}_t]\!]\} && \wr (14) \wr
\end{aligned}$$

$\mathring{\mathbb{E}}^i$ $\{\langle \ell, \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\} \cup \{\langle \ell, \overline{\rho}\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \overline{\rho}_{\mathtt{ff}}\rangle \mid \exists \overline{\rho}_{\mathtt{tt}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle \wedge \overline{\rho}_{\mathtt{ff}} \neq \dot{\varnothing}\} \cup \{\langle \ell, \overline{\rho}\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi} \mid \exists \overline{\rho}_{\mathtt{ff}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle \wedge \overline{\rho}_{\mathtt{tt}} \neq \dot{\varnothing} \wedge \langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi} \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_t]\!]\}$

〈— For the first term, by def. (18) of $\mathring{\mathbb{E}}^i$, we must prove that $\forall \rho \,.\, \exists \overline{\rho} \,.\, \langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mathrel{\dot{\sqsubseteq}}^i \langle \ell, \overline{\rho}\rangle$. Since $\{\dot{\alpha}^{\mathbb{I}}(\rho) \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{R}}\} \subseteq \mathbb{E}\mathbb{v}_{\mathbb{I}}$, we can simply choose $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$.

— The second term may be empty, in which case $\overline{\rho}_{\mathtt{ff}} = \dot{\varnothing}$. Otherwise, by def. (18) of $\mathring{\mathbb{E}}^i$, we must prove that $\forall \rho \,.\, \exists \overline{\rho} \,.\, \langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \dot{\alpha}^{\mathbb{I}}(\rho)\rangle \mathrel{\dot{\sqsubseteq}}^i \langle \ell, \overline{\rho}\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \overline{\rho}_{\mathtt{ff}}\rangle$. The control abstraction is the same. We can choose $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ so that $\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{ff}$ implies, by (22), that $\dot{\alpha}^{\mathbb{I}}(\rho) \mathrel{\dot{\sqsubseteq}}^i \overline{\rho}_{\mathtt{ff}}$.

— The third term may be empty, in which case $\overline{\rho}_{\mathtt{tt}} = \dot{\varnothing}$. Otherwise, by def. (18) of $\mathrel{\dot{\sqsubseteq}}^i$, we must prove that $\forall \rho, \pi \,.\, \exists \overline{\rho}, \overline{\pi} \,.\, \langle \ell, \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\alpha^{\mathbb{I}}(\pi) \mathrel{\dot{\sqsubseteq}}^i \langle \ell, \overline{\rho}\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}$ where $\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}$, $\langle \mathsf{at}[\![\mathtt{S}_t]\!], \rho\rangle\pi \in \mathscr{S}^*_{\mathbb{R}}[\![\mathtt{S}_t]\!]$, $\mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle$, and $\langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi} \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_t]\!]$.

The control abstraction is the same. We can choose $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ so that $\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}$ implies, by (22), that $\dot{\alpha}^{\mathbb{I}}(\rho) \mathrel{\dot{\sqsubseteq}}^i \overline{\rho}_{\mathtt{tt}} \mathrel{\dot{\sqsubseteq}}^i \overline{\rho}$ so that $\dot{\alpha}^{\mathbb{I}}(\rho) = \overline{\rho}_{\mathtt{tt}}$ since $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$.

It remains to find $\overline{\pi}$ such that $\alpha^{\mathbb{I}}(\pi) \mathrel{\dot{\sqsubseteq}}^i \overline{\pi}$ and $\langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi} \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_t]\!]$. It is given by (20) where $\langle \mathsf{at}[\![\mathtt{S}_t]\!], \rho\rangle\pi \in \mathscr{S}^*_{\mathbb{R}}[\![\mathtt{S}_t]\!]$ implies for $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ that $\exists \overline{\pi} \,.\, \alpha^{\mathbb{I}}(\pi) \mathrel{\dot{\sqsubseteq}}^i \overline{\pi} \wedge \langle \mathsf{at}[\![\mathtt{S}]\!], \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\overline{\pi} \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}]\!]$. It follows that $\alpha^{\mathbb{I}}(\pi) \mathrel{\dot{\sqsubseteq}}^i \overline{\pi}$ and $\langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi} \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_t]\!]$ since $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$. 〉

$\triangleq$ $\mathscr{S}^*_{\mathbb{I}}[\![\mathtt{if}\ \ell\ (\mathtt{B})\ \mathtt{S}_t]\!]$

〈since the above term involves only computations in $\mathbb{S}_{\mathbb{I}}$ and none in $\mathbb{S}_{\mathbb{V}}$〉

It remains to show that $\mathscr{S}^*_{\mathbb{I}}[\![\mathtt{if}\ \ell\ (\mathtt{B})\ \mathtt{S}_t]\!]$ satisfies (20), which is trivial for the first two terms. For the third term, this follows from the induction hypothesis. □

By calculational design, we have got the interval test as follows

$$\begin{aligned}\mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}]\!] \triangleq\ & \{\langle \ell, \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{I}}\} \\ & \cup \{\langle \ell, \overline{\rho}\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \overline{\rho}_{\mathtt{ff}}\rangle \mid \exists \overline{\rho}_{\mathtt{tt}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle \wedge \rho_{\mathtt{ff}} \neq \dot{\varnothing}\} \\ & \cup \{\langle \ell, \overline{\rho}\rangle\langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\pi \mid \exists \overline{\rho}_{\mathtt{ff}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle \wedge \rho_{\mathtt{tt}} \neq \dot{\varnothing} \wedge \\ & \qquad\qquad \langle \mathsf{at}[\![\mathtt{S}_t]\!], \overline{\rho}_{\mathtt{tt}}\rangle\pi \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_t]\!]\}\end{aligned} \tag{5bis}$$

Most libraries raise an error exception in case of split (or chose only one branch) which we can formalize as an undefined behavior, à la C, where any behavior is possible.

$$\begin{aligned}\mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}]\!] \triangleq\ & \cdots \\ & \cup \{\langle \ell, \overline{\rho}\rangle\pi \mid \exists \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle \wedge \rho_{\mathtt{tt}} \mathbin{\dot{\sqcap}^i} \rho_{\mathtt{ff}} \neq \dot{\varnothing} \wedge \pi \in \mathbb{S}^{+\infty}_{\mathbb{I}}\}\end{aligned} \tag{5.ter}$$

Fixpoint approximation For the iteration statement, we rely on the following fixpoint abstraction theorem (adapted from the more general [9, Prop. 2]).

Theorem 1 (least fixpoint over-approximation in a cpo). *Assume that* $\langle C, \sqsubseteq, \bot, \sqcup\rangle$ *is a cpo,* $f \in C \xrightarrow{uc} C$ *is* $\sqcup$*-upper continuous,* $\mathcal{I} \in \wp(C)$ *contains the*

iterates $f^0(\bot) = \bot$ *and* $f^{n+1}(\bot) = f(f^n(\bot))$ *of* f *from* $\bot$, $\langle \mathcal{A}, \preccurlyeq, 0, \curlyvee \rangle$ *is a cpo,* $\overline{f} \in \mathcal{A} \xrightarrow{uc} \mathcal{A}$ *is* $\curlyvee$*-upper continuous,* $\trianglelefteq$ *is a preorder on* $\mathcal{A}$, $\alpha \in C \to \mathcal{A}$, $\alpha(\bot) \trianglelefteq 0$, $\forall x \in \mathcal{I}, y \in \mathcal{A} \,.\, (\alpha(x) \trianglelefteq y) \Rightarrow (\alpha(f(x)) \trianglelefteq \overline{f}(y))$, *and for all* $\sqsubseteq$*-increasing chains* $\langle x^i, i \in \mathbb{N} \rangle$ *of* $\mathcal{I}$ *and* $\preccurlyeq$*-increasing chains* $\langle y^i, i \in \mathbb{N} \rangle$ *of* $\mathcal{A}$, $\alpha(\bigsqcup_{i \in \mathbb{N}} x^i) \trianglelefteq \bigvee_{i \in \mathbb{N}} y^i$. *Then* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \trianglelefteq \mathsf{lfp}^{\preccurlyeq} \overline{f}$. □

Remark 1. If $\overline{f}$ is $\trianglelefteq$-increasing, and $\forall x \in \mathcal{I} \,.\, \alpha \circ f(x) \trianglelefteq \overline{f} \circ \alpha(x)$ (semi-commutativity) then $\forall x \in \mathcal{I} \,.\, \alpha(x) \trianglelefteq y \Rightarrow \overline{f}(\alpha(x)) \trianglelefteq \overline{f}(y) \Rightarrow \alpha(f(x)) \trianglelefteq \overline{f}(y)$. Since, in general, this property does not hold for all $x \in C$ and it is used for the iterates of f only, $\mathcal{I} \in \wp(C)$ can be used to restrict the elements of C for which the property is required to hold. □

Proof (of Th. 1). By Scott-Kleene fixpoint, $f \in C \xrightarrow{uc} C$ is $\sqcup$-continuous function on a cpo $\langle C, \sqsubseteq, \bot, \sqcup \rangle$ so f has a least fixpoint $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcup_{n \in \mathbb{N}} f^n(\bot)$. Similarly, $\mathsf{lfp}^{\preccurlyeq} \overline{f} = \bigvee_{n \in \mathbb{N}} \overline{f}^n(0)$. We have $\alpha(f^0(\bot)) = \alpha(\bot) \trianglelefteq 0 = \overline{f}^0(0)$. Then $f^n(\bot) \in \mathcal{I}$ and $\alpha(f^n(\bot)) \trianglelefteq \overline{f}^n(0)$ by ind. hyp. so that $\alpha(f^{n+1}(\bot)) = \alpha(f(f^n(\bot))) \trianglelefteq \overline{f}(\overline{f}^n(0)) = \overline{f}^{n+1}(0)$. By recurrence $\forall n \in \mathbb{N} \,.\, \alpha(f^n(\bot)) \trianglelefteq \overline{f}^n(0)$. Since the fixpoint iterates are increasing, it follows, by hypothesis, that $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \alpha(\bigsqcup_{n \in \mathbb{N}} f^n(\bot)) = \bigvee_{n \in \mathbb{N}} \overline{f}^n(0) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$. □

Interval trace semantics of the iteration statement We define $\mathcal{I}$ in Th. 1 by assuming that iterate X satisfies the induction hypothesis (20), which is trivially satisfied by the first iterate $\varnothing$.

$$
\begin{aligned}
& \mathring{\alpha}^{\mathbb{I}}(\mathscr{F}^*_{\mathbb{V}}[\![\texttt{while}^{\ell}\ \texttt{(B)}\ \mathsf{S}_b]\!]\, X) \\
= \; & \mathring{\alpha}^{\mathbb{I}}(\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}_{\mathbb{V}_{\mathbb{R}}}\} \cup \{\pi_2\langle \ell', \rho\rangle\langle \mathsf{aft}[\![\mathsf{S}]\!], \rho\rangle \mid \pi_2\langle \ell', \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathtt{ff} \wedge \ell' = \ell\} \cup \{\pi_2\langle \ell', \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \mid \pi_2\langle \ell', \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{R}}[\![\mathsf{S}_b]\!] \wedge \ell' = \ell\}) \qquad \text{(def (8) of } \mathscr{F}^*_{\mathbb{V}}[\![\texttt{while}^{\ell}\ \texttt{(B)}\ \mathsf{S}_b]\!]\text{)} \\
= \; & \mathring{\alpha}^{\mathbb{I}}(\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}_{\mathbb{V}_{\mathbb{R}}}\}) \cup \alpha^{\mathbb{I}}(\{\pi_2\langle \ell', \rho\rangle\langle \mathsf{aft}[\![\mathsf{S}]\!], \rho\rangle \mid \pi_2\langle \ell', \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathtt{ff} \wedge \ell' = \ell\}) \cup \alpha^{\mathbb{I}}(\{\pi_2\langle \ell', \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \mid \pi_2\langle \ell', \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{R}}[\![\mathsf{S}_b]\!] \wedge \ell' = \ell\}) \qquad \text{(join preservation in the Galois connection (15))}
\end{aligned}
$$

The first two terms have already been handled in the case of a conditional statement $\texttt{if}^{\ell}\ \texttt{(B)}\ \mathsf{S}_t$. It remains the third term (simplified with $\ell' = \ell$), which, in the non-empty case is as follows.

$$
\begin{aligned}
& \mathring{\alpha}^{\mathbb{I}}(\{\pi_2\langle \ell, \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \mid \pi_2\langle \ell, \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{R}}[\![\mathsf{S}_b]\!]\}) \\
= \; & \{\alpha^{\mathbb{I}}(\pi_2)\langle \ell, \mathring{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \mathring{\alpha}^{\mathbb{I}}(\rho)\rangle\alpha^{\mathbb{I}}(\pi_3) \mid \pi_2\langle \ell, \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{R}}[\![\mathsf{S}_b]\!]\} \qquad \text{(def. (14) of } \mathring{\alpha}^{\mathbb{I}}\text{)} \\
\mathring{\mathbb{E}}^i \; & \{\overline{\pi}_2\langle \ell, \overline{\rho}\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3) \mid \overline{\pi}_2\langle \ell, \overline{\rho}\rangle \in \alpha^{\mathbb{I}}(X) \wedge \exists \overline{\rho}_{\mathtt{ff}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathsf{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{I}}[\![\mathsf{S}_b]\!]\}
\end{aligned}
$$

⟅By def. (18) of $\mathring{\sqsubseteq}^i$, we must prove that $\vec{\alpha}^{\mathbb{I}}(\pi_2)\langle \ell,\ \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\vec{\alpha}^{\mathbb{I}}(\pi_3) \sqsubseteq^i \overline{\pi}_2\langle \ell,\ \overline{\rho}\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}\rangle\overline{\pi}_3)$ where $\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}$, $\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{R}}[\![\mathtt{S}_b]\!]$, $\mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle$, and $\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_b]\!]$.

The control abstraction is the same. We can choose $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ so that $\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}$ implies, by (22), that $\dot{\alpha}^{\mathbb{I}}(\rho) \mathrel{\dot{\sqsubseteq}}^i \overline{\rho}_{\mathtt{tt}} \mathrel{\dot{\sqsubseteq}}^i \overline{\rho}$ so that $\dot{\alpha}^{\mathbb{I}}(\rho) = \overline{\rho}_{\mathtt{tt}}$ since $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$.

We choose $\overline{\pi}_2 = \vec{\alpha}^{\mathbb{I}}(\pi_2)$ so that $\pi_2\langle \ell,\ \rho\rangle \in X$ implies, by def. (14) of $\alpha^{\mathbb{I}}$, that $\overline{\pi}_2\langle \ell, \overline{\rho}\rangle \in \mathring{\alpha}^{\mathbb{I}}(X)$ with $\vec{\alpha}^{\mathbb{I}}(\pi_2\langle \ell,\ \rho\rangle) \vec{\sqsubseteq}^i \overline{\pi}_2\langle \ell, \overline{\rho}\rangle$ since $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ and $\vec{\sqsubseteq}^i$ is reflexive.

It remains to find $\overline{\pi}_3$ such that $\vec{\alpha}^{\mathbb{I}}(\pi_3) \vec{\sqsubseteq}^i \overline{\pi}_3$ and $\langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_t]\!]$. It is given by (20) where $\langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \rho\rangle\pi_3 \in \mathscr{S}^*_{\mathbb{R}}[\![\mathtt{S}_b]\!]$ implies for $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ that $\exists \overline{\pi}_3\ .\ \vec{\alpha}^{\mathbb{I}}(\pi_3) \vec{\sqsubseteq}^i \overline{\pi}_3 \wedge \langle \mathsf{at}[\![\mathtt{S}]\!],\ \dot{\alpha}^{\mathbb{I}}(\rho)\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}]\!]$. It follows that $\vec{\alpha}^{\mathbb{I}}(\pi_3) \vec{\sqsubseteq}^i \overline{\pi}_3$ and $\langle \mathsf{at}[\![\mathtt{S}_t]\!],\ \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_b]\!]$ since $\overline{\rho} = \dot{\alpha}^{\mathbb{I}}(\rho)$ ⟆

Since the above terms involves only computations in $\mathbb{S}_{\mathbb{I}}$ and none in $\mathbb{S}_{\mathbb{V}}$, we can define (again an undefined behavior can be introduced for overlapping tests)

$$
\begin{aligned}
\mathscr{F}^*_{\mathbb{I}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]\ X \triangleq\ & \{\langle \ell,\ \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathsf{v}_{\mathbb{I}}\} \qquad (8\text{bis})\\
& \cup \{\overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!],\ \overline{\rho}_{\mathtt{ff}}\rangle \mid\\
& \qquad \overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle \in X \wedge \exists \overline{\rho}_{\mathtt{tt}}\ .\ \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge \overline{\rho}_{\mathtt{ff}} \neq \dot{\varnothing} \wedge \ell' = \ell\}\\
& \cup \{\overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}\rangle\overline{\pi}_3 \mid \overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle \in X \wedge\\
& \quad \exists \overline{\rho}_{\mathtt{ff}}\ .\ \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge \overline{\rho}_{\mathtt{tt}} \neq \dot{\varnothing} \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{I}}[\![\mathtt{S}_b]\!] \wedge \ell' = \ell\}
\end{aligned}
$$

so that $\mathring{\alpha}^{\mathbb{I}}(\mathscr{F}^*_{\mathbb{R}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]X) = \mathscr{F}^*_{\mathbb{I}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!](\alpha^{\mathbb{I}}(X))$. We have to show that the next iterate $\mathscr{F}^*_{\mathbb{I}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]\ X$ satisfies (20), which is trivial for the first two terms. For the third term this follows from the induction hypothesis. It follows that

$$
\begin{aligned}
\mathscr{S}^*_{\mathbb{I}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!] &= \mathring{\alpha}^{\mathbb{I}}(\mathscr{S}^*_{\mathbb{R}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]) && ⟅\text{by def.}⟆ \qquad (23)\\
&= \mathring{\alpha}^{\mathbb{I}}(\mathsf{lfp}^{\subseteq}\ \mathscr{F}^*_{\mathbb{R}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]) && ⟅\text{by (8)}⟆\\
&\mathrel{\mathring{\sqsubseteq}}^i \mathsf{lfp}^{\subseteq}\ \mathscr{F}^*_{\mathbb{I}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!] && ⟅\text{by Th. 1}⟆
\end{aligned}
$$

It remains to show that $\mathscr{S}^*_{\mathbb{I}}[\![\mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b]\!]$ satisfies (20). We have shown that it holds for all fixpoint iterates. Moreover, it is trivially preserved by trace set union. □

In conclusion of this section, $\mathscr{S}^*_{\mathbb{I}}$ is similar to $\mathscr{S}^*_{\mathbb{V}}$ in (2)—(7) except for statements involving tests for which we have (5bis) or (5ter) and (8bis).

8 On floating point computations

Unfortunately real computations are usually performed using floating point arithmetics. One computes only one floating point value hoping it is not too far from the real one. This problem has been deeply studied in static analysis [10,11,13,15,16,18,19,20,17,29]. Another dynamic analysis solution is to check the precision with an interval analysis.

Consider the execution with reals (at least their semantics), floats and float intervals, maybe with different possible execution traces for float intervals due to the nondeterminacy of tests. These interval executions abstract both the real and float executions.

If there is only one interval execution trace or we can prove that the real and float executions follow exactly the same control path then the real execution is in the join of the interval executions to which the float execution belongs to, when projected on all program points.

Otherwise, the real and float executions may have followed different paths but both are guaranteed to belong to the union of all interval executions projected on all program points.

In both cases this provides an estimate of the rounding error of the float execution compared to the ideal real execution. Of course the estimate might be rough since specific properties of the computation are not taken into account (*e.g.* [25, pp. 91–94]).

9 Abstraction to a transition system

One could argue that a sound maximal trace semantics of interval arithmetics does not describe an implementation. However, we can abstract to a small-step operational semantics that is a transition system describing elementary steps of an implementation.

A transition system is a triple $\langle \Sigma,\ \mathrm{I},\ \xrightarrow{\tau} \rangle$ where Σ is a non-empty set of states σ, $\mathrm{I} \subseteq \Sigma$ is a set of initial states, and $\xrightarrow{\tau} \in \wp(\Sigma \times \Sigma)$ is a transition relation between a state and its possible successors.

A transition system $\langle \Sigma,\ \mathrm{I},\ \xrightarrow{\tau} \rangle$ can be used to define a state prefix trace semantics as follows.

$$\gamma^{\tau}(\langle \Sigma,\ \mathrm{I},\ \xrightarrow{\tau} \rangle) \triangleq \{\pi_0 \cdot \cdots \cdot \pi_n \mid n \in \mathbb{N} \wedge \pi_0 \in \mathrm{I} \wedge \forall i \in [0, n[\ .\ \pi_i \xrightarrow{\tau} \pi_{i+1}\} \quad (24)$$

(where $\sigma \xrightarrow{\tau} \sigma'$ is a shorthand for $\langle \sigma,\ \sigma' \rangle \in \xrightarrow{\tau}$.)

Conversely a prefix trace semantics S can be abstracted in a transition system

$$\alpha^{\tau}(S) \triangleq \langle \Sigma,\ \mathrm{I},\ \xrightarrow{\tau} \rangle \quad (25)$$

where

$$\begin{aligned}
\Sigma &\triangleq \{\pi_i \mid \exists n \in \mathbb{N}, \pi_0, \ldots, \pi_{i-1}, \pi_{i+1}, \ldots, \pi_n\ .\ \pi_0 \cdots \pi_n \in S\} \qquad (\text{or } \mathbb{S}) \\
\mathrm{I} &\triangleq \{\pi_0 \mid \exists n \in \mathbb{N}, \pi_1, \ldots, \pi_n\ .\ \pi_0 \cdots \pi_n \in S\} \\
\xrightarrow{\tau} &\triangleq \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n\ .\ \pi_0 \cdots \pi_n \in S\}
\end{aligned}$$

This is a Galois connection

$$\langle \wp(\mathbb{T}^+),\ \subseteq \rangle \underset{\alpha^{\tau}}{\overset{\gamma^{\tau}}{\leftrightarrows}} \langle \{\langle \Sigma,\ \mathrm{I},\ \xrightarrow{\tau} \rangle \mid \Sigma \in \wp(\mathbb{S}) \wedge \mathrm{I} \subseteq \Sigma \wedge \xrightarrow{\tau} \subseteq \Sigma \times \Sigma\},\ \dot{\subseteq} \rangle$$

In general information is lost by the abstraction of a prefix trace semantics to a transition system (take for example $\Pi = \{a, aa\}$ so that $\gamma^\tau \circ \alpha^\tau(\Pi) = a^+$ is the set of all non-empty finite sequences of "a"s). However, this is not the case since the maximal semantics has been defined as the limit of prefix-closed traces, finite maximal final traces are not strict prefixes of any other trace, and so, final states have no possible successor.

Notice that the abstraction of the prefix trace semantics of a program into a transition system will only comprehend reachable states. So the transition semantics for a language is the join of all transition systems of the prefix trace semantics of all programs in the semantics. This may still be a strict overapproximation.

The transition semantics of the programming language $\mathbb{P}$ with program components $\mathbb{P}\mathbb{c}$ is

$$\alpha^\tau(\mathcal{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]) = \langle \mathbb{S}, \{\langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \mid \mathtt{S} \in \mathbb{P}\mathbb{c} \wedge \rho \in \mathbb{E}\mathbb{v}\}, \widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{S}]\!]\rangle$$

defined by structural induction on program components $\mathtt{S} \in \mathbb{P}\mathbb{c}$ as follows.

9.1 Transition semantics of an assignment statement $\mathtt{S} ::= \ell\ \mathtt{x = A\ ;}$

$$\widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{S}]\!] = \{\langle \ell, \rho\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!], \rho[\mathtt{x} \leftarrow \mathcal{A}[\![\mathtt{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \tag{26}$$

Proof (of (26)).

$$\begin{aligned}
&\widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{S}]\!]\\
&= \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\} && \wr(25)\wr\\
&= \{\langle \ell, \rho\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!], \rho[\mathtt{x} \leftarrow \mathcal{A}[\![\mathtt{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} && \wr(2)\wr \quad \square
\end{aligned}$$

9.2 Transition semantics of a statement list $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$

$$\widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{Sl}]\!] = \widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{Sl}']\!] \cup \widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{S}]\!] \tag{27}$$

Proof (of (27)).

$$\begin{aligned}
&\widehat{\mathcal{S}}^\tau_{\mathbb{V}}[\![\mathtt{Sl}]\!]\\
&= \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}]\!]\} && \wr(25)\wr\\
&= \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!] \cup \{\pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!],\\
&\quad \rho\rangle \cdot \pi' \mid \pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!] \wedge \langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \cdot \pi' \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\}\} && \wr\text{def. (7) of } \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}]\!]\wr\\
&= \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!]\} \cup \{\pi_i \longrightarrow\\
&\quad \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \{\pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \cdot \pi' \mid \pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!],\\
&\quad \rho\rangle \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!] \wedge \langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \cdot \pi' \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\}\} && \wr\text{def. } \cup\wr\\
&= \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!]\} \cup \{\pi_i \longrightarrow\\
&\quad \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \{\langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \cdot \pi' \mid \langle \mathsf{at}[\![\mathtt{S}]\!],\\
&\quad \rho\rangle \cdot \pi' \in \mathcal{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\}\}
\end{aligned}$$

$\wr$since all transitions originating from $\pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle = \pi \cdot \langle \mathsf{aft}[\![\mathtt{Sl}']\!],\ \rho\rangle \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!]$ have already been collected in the first term of the $\cup\int$

$= \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{Sl}']\!]\} \cup \{\pi_i \longrightarrow \pi_{i+1} \mid \exists n \in \mathbb{N}_*, \pi_0, \ldots, \pi_{i-1}, \pi_{i+2}, \ldots, \pi_n \,.\, \pi_0 \cdots \pi_n \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\}$

$\wr$since all traces of $\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ start with state $\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\int$

$= \widehat{\mathscr{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}']\!] \cup \widehat{\mathscr{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]$ $\wr$(25) and ind. hyp. $\int$ □

9.3 Transition semantics of an iteration statement $\mathtt{S} ::= \mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b$ and a break statement $\mathtt{S} ::= \ell\ \mathtt{break}\ \mathtt{;}$

Real ($\mathbb{V} = \mathbb{R}$) and float ($\mathbb{V} = \mathbb{F}$) semantics.

$$\widehat{\mathscr{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!] = \{\langle \ell,\ \rho\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!],\ \rho\rangle \mid \mathscr{B}[\![\mathtt{B}]\!]\,\rho = \mathtt{ff}\} \cup \{\langle \ell,\ \rho\rangle \longrightarrow \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle \mid \mathscr{B}[\![\mathtt{B}]\!]\,\rho = \mathtt{tt}\} \cup \widehat{\mathscr{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}_b]\!] \tag{28}$$

$$\widehat{\mathscr{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{break}\ \mathtt{;}]\!] = \{\langle \ell,\ \rho\rangle \longrightarrow \langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathrm{v}_{\mathbb{V}}\} \tag{29}$$

By definition of $\mathsf{aft}[\![\mathtt{S}_b]\!] = \mathsf{at}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!] = \ell$, there is no need for a transition from after the loop body $\mathtt{S}_b$ to the start ℓ of the loop.

Float interval ($\mathbb{V} = \mathbb{I}$) semantics. For float intervals, the transition is non-deterministic.

$$\widehat{\mathscr{S}}^{\tau}_{\mathbb{I}}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!] = \{\langle \ell,\ \overline{\rho}\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!],\ \overline{\rho}_{\mathtt{ff}}\rangle \mid \exists \overline{\rho}_{\mathtt{tt}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\} \cup \{\langle \ell,\ \overline{\rho}\rangle \longrightarrow \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}_{\mathtt{tt}}\rangle \mid \exists \overline{\rho}_{\mathtt{ff}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\} \cup \widehat{\mathscr{S}}^{\tau}_{\mathbb{I}}[\![\mathtt{S}_b]\!] \tag{30}$$

Proof (of (30)). (The proof of (28) and (29) is similar).

$\widehat{\mathscr{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]$ $\wr$where $\mathtt{S} ::= \mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b\int$

$= \{\overline{\pi}_i \longrightarrow \overline{\pi}_{i+1} \mid \exists n \in \mathbb{N}_*, \overline{\pi}_0, \ldots, \overline{\pi}_{i-1}, \overline{\pi}_{i+2}, \ldots, \overline{\pi}_n \,.\, \overline{\pi}_0 \cdots \overline{\pi}_n \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\}$ $\wr$(25)$\int$

$= \{\langle \ell_i, \overline{\rho}_i\rangle \longrightarrow \langle \ell_{i+1}, \overline{\rho}_{i+1}\rangle \mid \exists n \in \mathbb{N}_*, \langle \ell_0, \overline{\rho}_0\rangle, \ldots, \langle \ell_{i-1}, \overline{\rho}_{i-1}\rangle, \langle \ell_{i+2}, \overline{\rho}_{i+2}\rangle, \ldots, \langle \ell_n, \overline{\rho}_n\rangle \,.\, \langle \ell_0, \overline{\rho}_0\rangle \cdots \langle \ell_n, \overline{\rho}_n\rangle \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]\}$ $\wr$def. (2)—(4), (5bis), ((6)), (7), (8bis) of $\mathscr{S}^*_{\mathbb{V}}\int$

Following the fixpoint definition of $\mathscr{S}^*_{\mathbb{V}}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]$, we have to collect the transitions after 0 or one more iteration in (8bis), so the proof is on the number of fixpoint iterations of $\mathscr{F}^*_{\mathbb{I}}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]\ X$, knowing that, by induction, the transitions of all traces in X have already been collected.

- For the basis, $\{\langle \ell,\ \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathrm{v}_{\mathbb{I}}\}$ yields no transition;
- $\{\overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!],\ \overline{\rho}_{\mathtt{ff}}\rangle \mid \overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle \in X \wedge \exists \overline{\overline{\rho}}_{\mathtt{tt}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\overline{\rho}} = \langle \overline{\overline{\rho}}_{\mathtt{tt}},\ \overline{\overline{\rho}}_{\mathtt{ff}}\rangle \wedge \ell' = \ell\}$ yields transitions $\{\langle \ell,\ \overline{\rho}\rangle \longrightarrow \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}_{\mathtt{ff}}\rangle \mid \exists \overline{\overline{\rho}}_{\mathtt{tt}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\overline{\rho}} = \langle \overline{\overline{\rho}}_{\mathtt{tt}},\ \overline{\overline{\rho}}_{\mathtt{ff}}\rangle\}$. The transitions of $\overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle \in X$ have already been collected. $\overline{\rho}$ can be chosen arbitrarily for the converse inclusion;
- $\{\overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3 \mid \overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle \in X \wedge \exists \overline{\overline{\rho}}_{\mathtt{ff}} \,.\, \mathscr{B}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\overline{\rho}} = \langle \overline{\overline{\rho}}_{\mathtt{tt}},\ \overline{\overline{\rho}}_{\mathtt{ff}}\rangle \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3 \in \mathscr{S}^*_{\mathbb{V}}[\![\mathtt{S}_b]\!] \wedge \ell' = \ell\}$ yields the transitions of $\overline{\pi}_2\langle \ell',\ \overline{\rho}\rangle \in X$ which have already been collected by induction on the iterates, the transitions of $\langle \mathsf{at}[\![\mathtt{S}_b]\!],$

$\overline{\rho}_{\mathtt{tt}}\rangle\overline{\pi}_3 \in \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}_b]\!]$ which have already been collected in $\widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}_b]\!]$ by structural induction, plus the transitions $\{\langle \ell, \overline{\rho}\rangle \longrightarrow \langle \mathsf{at}[\![\mathtt{S}_b]\!], \overline{\rho}_{\mathtt{tt}}\rangle \mid \exists \overline{\rho}_{\mathtt{ff}} \,.\, \boldsymbol{\mathcal{B}}_{\mathbb{I}}[\![\mathtt{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle\}$. □

The transition semantics of a program $\mathtt{P} ::= \mathtt{Sl}\ \ell$, an empty statement list $\mathtt{Sl} ::= \epsilon$, a skip statement $\mathtt{S} ::= \ell\mathtt{;}$, conditional statements $\mathtt{S} ::= \mathtt{if}\ \ell\ \mathtt{(B)}\ \mathtt{S}_t$ and $\mathtt{S} ::= \mathtt{if}\ \ell\ \mathtt{(B)}\ \mathtt{S}_t\ \mathtt{else}\ \mathtt{S}_f$, and a compound statement $\mathtt{S} ::= \mathtt{\{\ Sl\ \}}$. are similar.

9.4 The transition semantics generates the trace semantics

Theorem 2. *The prefix trace semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}$ of Sections 2 and 7 is generated by the transition semantics $\widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}$ of Section 9.*

Proof (of Th. 2). The proof is by structural induction on the program components $\mathtt{S} \in \mathcal{PC}$ of the language $\mathcal{P}$. Let $\langle \mathbb{S}, \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!], \mathrm{I}[\![\mathtt{S}]\!]\rangle$ where $\mathrm{I}[\![\mathtt{S}]\!] \triangleq \{\langle \mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\}$ be the transition system of the program components $\mathtt{S}$, as defined in Section 9. Let $\boldsymbol{\mathcal{S}}^*(\langle \mathbb{S}, \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!], \mathrm{I}[\![\mathtt{S}]\!]\rangle)$ be the set of stateful prefix traces generated by this transition system, as defined in (24). We must show that $\boldsymbol{\mathcal{S}}^*(\langle \mathbb{S}, \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!], \mathrm{I}[\![\mathtt{S}]\!]\rangle) = \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ for the structural stateful prefix semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ defined in Sections **2** and **7**.

– We observe that traces of length 1 in $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ are all of the form $\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\}$ which are exactly the same for $n = 0$ is (24). So, in the following, we just have to consider prefix traces of length strictly greater than 1.

– For the assignment statement $\mathtt{S} ::= \ell\ \mathtt{x = A\ ;}$, we have

$$\{\pi_0 \cdot \cdots \cdot \pi_n \mid n \in \mathbb{N} \wedge \pi_0 \in \mathrm{I}[\![\mathtt{S}]\!] \wedge \forall i \in [0, n[\ .\ \langle \pi_i, \pi_{i+1}\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]\} \qquad \wr(24)\wr$$

$$= \{\pi_0 \cdot \cdots \cdot \pi_n \mid n \in \mathbb{N} \wedge \pi_0 \in \mathrm{I}[\![\mathtt{S}]\!] \wedge \forall i \in [0, n[\ .\ \langle \pi_i, \pi_{i+1}\rangle \in \{\langle \ell, \rho\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!], \boldsymbol{\mathcal{A}}[\![\mathtt{A}]\!]\rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\}\} \qquad \wr(26)\wr$$

$$= \{\pi_0\pi_1 \mid \langle \pi_0, \pi_1\rangle \in \{\langle \ell, \rho\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!], \boldsymbol{\mathcal{A}}[\![\mathtt{A}]\!]\rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\}\}$$
$$\wr\text{since } \ell = \mathsf{at}[\![\mathtt{S}]\!] \neq \mathsf{aft}[\![\mathtt{S}]\!] \text{ and } \pi_0 = \langle \ell, \rho\rangle \in \mathrm{I}[\![\mathtt{S}]\!] \text{ by def. } \mathrm{I}[\![\mathtt{S}]\!]\wr$$

$$= \{\langle \ell, \rho\rangle\langle \mathsf{aft}[\![\mathtt{S}]\!], \boldsymbol{\mathcal{A}}[\![\mathtt{A}]\!]\rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \qquad \wr\text{def. } \in\wr$$

$$= \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!] \setminus \{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \qquad \wr(2)\wr$$

so we conclude that (24) generates $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ since in the proof we have left apart the trivial case of traces $\{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\}$ of length 1.

– For the statement list $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$, we have

$$\{\pi_0 \cdot \cdots \cdot \pi_n \mid n \in \mathbb{N} \wedge \pi_0 \in \mathrm{I}[\![\mathtt{Sl}]\!] \wedge \forall i \in [0, n[\ .\ \langle \pi_i, \pi_{i+1}\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}]\!]\} \qquad \wr(24)\wr$$

$$= \{\pi_0 \cdot \cdots \cdot \pi_n \mid n \in \mathbb{N} \wedge \pi_0 \in \mathrm{I}[\![\mathtt{Sl}]\!] \wedge \forall i \in [0, n[\ .\ \langle \pi_i, \pi_{i+1}\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}']\!] \cup \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]\} \qquad \wr(27)\wr$$

$$= \{\pi'_0 \cdot \cdots \cdot \pi'_{n'} \mid n' \in \mathbb{N} \wedge \pi'_0 \in \mathrm{I}[\![\mathtt{Sl}]\!] \wedge \forall i \in [0, n'[\ .\ \langle \pi'_i, \pi'_{i+1}\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}']\!]\} \cup \{\pi'_0 \cdot \cdots \cdot \pi'_{n'} \frown \pi''_0 \cdot \cdots \cdot \pi''_m \mid n' \in \mathbb{N} \wedge \pi'_0 \in \mathrm{I}[\![\mathtt{Sl}]\!] \wedge \forall i \in [0, n'[\ .\ \langle \pi'_i, \pi'_{i+1}\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}']\!] \wedge m \in \mathbb{N} \wedge \pi''_0 \in \mathrm{I}[\![\mathtt{S}]\!] \wedge \forall i \in [0, m[\ .\ \langle \pi''_i, \pi''_{i+1}\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]\}$$

⁅since all states involved in $\langle \ell,\ \rho\rangle \in \widehat{\mathcal{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}']\!]$ have $\ell \in \mathsf{labs}[\![\mathtt{Sl}']\!]$ and similarly all states involved in $\langle \ell,\ \rho\rangle \in \widehat{\mathcal{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]$ have $\ell \in \mathsf{labs}[\![\mathtt{S}]\!]$ and $\pi_0 = \pi'_0 \in \mathrm{I}[\![\mathtt{Sl}]\!] = \mathrm{I}[\![\mathtt{Sl}']\!]$ so that $\mathsf{labs}[\![\mathtt{Sl}']\!] \cap \mathsf{labs}[\![\mathtt{S}]\!] = \{\mathsf{aft}[\![\mathtt{Sl}']\!]\} = \{\mathsf{at}[\![\mathtt{S}]\!]\}$ implies that the first transitions in $\pi'_0 \cdot \cdots \cdot \pi'_{n'}$ from $\pi_0 = \pi'_0$ must be transitions in $\widehat{\mathcal{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{Sl}']\!]$.
Then there are two cases. The first case is when $\pi'_0 \cdot\cdots\cdot \pi'_{n'}$ never reaches a final state of $\pi'_{n'} \neq \pi''_0$ of $\mathtt{Sl}'$ so that $\pi'_0 \cdot\cdots\cdot \pi'_{n'} = \pi_0 \cdot\cdots\cdot \pi_n$. Otherwise, a final state $\pi'_{n'} = \pi''_0$ is reached for which $\ell = \mathsf{aft}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$ so $\pi'_0 \cdot \cdots \cdot \pi'_{n'} \frown \pi''_0 \cdot \cdots \cdot \pi''_m = \pi_0 \cdot \cdots \cdot \pi_n$ since after $\pi'_{n'} = \pi''_0$ the transitions in $\pi''_0 \cdot \cdots \cdot \pi''_m$, if any when $m > 0$, must belong to $\widehat{\mathcal{S}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}]\!]$.
Both cases includes the empty statement list $\mathtt{Sl}' ::= \epsilon$ for which $n' = 0$⁆

$= \mathcal{S}^{*}_{\mathbb{V}}[\![\mathtt{Sl}']\!] \cup \{\pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \cdot \pi' \mid \pi \cdot \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \in \mathcal{S}^{*}_{\mathbb{V}}[\![\mathtt{Sl}']\!] \wedge \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \cdot \pi' \in \mathcal{S}^{*}_{\mathbb{V}}[\![\mathtt{S}]\!]\}$
⁅ind. hyp. ⁆

$= \mathcal{S}^{*}_{\mathbb{V}}[\![\mathtt{Sl}]\!]$ ⁅(7)⁆ □

– For the iteration statement $\mathtt{S} ::= \mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b$, we use the fact the prefix traces with entry label $\ell = \mathsf{at}[\![\mathtt{S}]\!] = \mathsf{aft}[\![\mathtt{S}_b]\!]$ have the form

$$\pi(n)\pi'(n) \in \widehat{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{S}]\!] \tag{31}$$

where

– $\pi(n) \triangleq \left(\langle \ell,\ \rho_i\rangle \xrightarrow{B} \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_i\rangle\pi(i)\langle \ell,\ \rho_{i+1}\rangle\right)_{i=1}^{n-1}$ is the trace of the first $n \geqslant 0$ iterations (reduced to $\langle \ell,\ \rho_0\rangle$ for $n = 0$) such that $\forall i \in [1, n-1]\ .\ \left(\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_i\rangle\pi(i)\langle \ell,\ \rho_{i+1}\rangle\right)_{i=1}^{n-1}$ is the maximal finite trace of the i-th iteration in the loop body $\mathtt{S}_b$;
– $\ell\pi'(n)$ traces the prefix execution of the n-th iteration in the loop body $\mathtt{S}_b$ or a loop exit, so

$$\begin{aligned}
\ell\pi'(n) \in\ & \{\langle \ell,\ \rho_n\rangle\} \cup \{\langle \ell,\ \rho_n\rangle \xrightarrow{B} \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_n\rangle \mid \mathcal{B}[\![\mathtt{B}]\!]\rho_n = \mathtt{tt}\} \\
& \cup \{\langle \ell,\ \rho_n\rangle \xrightarrow{\neg(\mathtt{B})} \langle \mathsf{aft}[\![\mathtt{S}]\!],\ \rho_n\rangle \mid \mathcal{B}[\![\mathtt{B}]\!]\rho_n = \mathtt{ff}\} \\
& \cup \{\langle \ell,\ \rho_n\rangle \xrightarrow{B} \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_n\rangle\pi''(n) \mid \\
& \qquad \mathcal{B}[\![\mathtt{B}]\!]\rho_n = \mathtt{tt} \wedge \langle \ell,\ \rho_n\rangle \xrightarrow{B} \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_n\rangle\pi''(n) \in \widehat{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{S}_b]\!]\} \\
& \cup \{\langle \ell,\ \rho_n\rangle \xrightarrow{\mathtt{B}} \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_n\rangle\pi_3 \xrightarrow{\mathtt{break}} \langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!],\ \rho_m\rangle \mid \mathcal{B}[\![\mathtt{B}]\!]\rho_n = \mathtt{tt} \wedge \\
& \qquad \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho_n\rangle\pi_3 \xrightarrow{\mathtt{break}} \langle \mathsf{brk\text{-}to}[\![\mathtt{S}]\!],\ \rho_m\rangle \in \widehat{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathtt{S}_b]\!]\}
\end{aligned}$$

Obviously the traces in (31) can be generated by the transition system.

Conversely, let $\langle \ell_0,\ \rho_0\rangle \cdots \langle \ell_n,\ \rho_n\rangle$ be a trace generated by the transition system for an iteration $\mathtt{S}$ so that $\ell_0 = \mathsf{at}[\![\mathtt{S}]\!]$. By reductio ad absurdum, let $k < n$ such that $\langle \ell_0,\ \rho_0\rangle \cdots \langle \ell_k,\ \rho_k\rangle$ is in $\mathcal{S}^{*}_{\mathbb{V}}[\![\mathtt{S}]\!]$ but $\langle \ell_0,\ \rho_0\rangle \cdots \langle \ell_k,\ \rho_k\rangle\langle \ell_{k+1},\ \rho_{k+1}\rangle$ is not. By recurrence, there exists $\pi_k\ell_k$ such that $\rho_k = \varrho(\pi_0\ell_0 \frown \pi_k\ell_k)$. Since we have the transition $\langle \ell_k,\ \rho_k\rangle \longrightarrow \langle \ell_{k+1},\ \rho_{k+1}\rangle$ there is one statement $\mathtt{S}'$ in Section 9 from

which this transition comes from such that $\ell_k \in \mathsf{labs}[\![\mathtt{S}']\!]$. The contradiction is that a similar step is possible in $\in \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$. We have to go on by considering all possible cases for $\mathtt{S}'$. Since the reasoning is similar for all these cases, let us consider the typical cases (26) and (28).

In case (26), ℓ_k is at an assignment statement $\mathtt{S}' ::= \ell\ \mathtt{x = A\ ;}$. Because of unicity of the labelling, the transition $\langle \ell_k, \rho_k\rangle \longrightarrow \langle \ell_{k+1}, \rho_{k+1}\rangle$ in (26) cannot come from any other statement. The contradiction is that (2) provides a transition in $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ that abstracts to the desired transition $\langle \ell_k, \rho_k\rangle \longrightarrow \langle \ell_{k+1}, \rho_{k+1}\rangle$.

The reasoning is the same in case (28) for $\{\langle \ell, \rho\rangle \longrightarrow \langle \mathsf{aft}[\![\mathtt{S}]\!], \rho\rangle \mid \boldsymbol{\mathcal{B}}[\![\mathtt{B}]\!]\,\rho = \mathtt{ff}\}$ and $\{\langle \ell, \rho\rangle \longrightarrow \langle \mathsf{at}[\![\mathtt{S}_b]\!], \rho\rangle \mid \boldsymbol{\mathcal{B}}[\![\mathtt{B}]\!]\,\rho = \mathtt{tt}\}$. Otherwise, $\ell_k \in \mathsf{labs}[\![\mathtt{S}_b]\!]$ and we consider recursively the contradiction within $\mathtt{S}' = \widehat{\boldsymbol{\mathcal{S}}}^{\tau}_{\mathbb{V}}[\![\mathtt{S}_b]\!]$. The reasoning is the same for the float interval semantics. □

It follows from Th. 2 that we could have followed the traditional way of defining a small-step operational semantics by first postulating the transition semantics of Section **9**, then deriving the stateful prefix trace semantics by (24), and finally deriving the maximal trace semantics by taking limits as in (9) and (10).

10 Conclusion

Dynamic interval analysis can be extended to ball analysis (also known as midpoint-radius interval arithmetic) [39,40].

Most applications of dynamic interval analysis involve tests (including the loop condition) on intervals but consider only the deterministic case where only one branch is taken. For example interval libraries raise an exception when more than one alternative should be taken in tests [2]. This can be understood as a trivial widening to all possible continuations after the test. When expressed as a transition system, the choice can be implemented *e.g.* by backtracking, which is natural in logic or constraint programming [35,36,38].

Our formalization of the float interval semantics as an abstraction of the real semantics uses an approximation preorder $\mathring{\sqsubseteq}^{i}$ different from the fixpoint ordering $\subseteq$ (also called computational ordering). This is a rare example in abstract interpretation with [9,34].

Dynamic interval analysis is different from other instrumented dynamic analyses for runtime verification [1,12,21,22] in that it does collect interval information upon executions, but does not check the collected information against a specification. Instead it replaces that execution (on reals or floats) by another one (on float intervals).

More generally, runtime verification of single executions collects information on the execution to check the execution against a formal specification, or to protect against errors [23]. Since only safety properties can be checked at runtime, this instrumented semantics can be formalized by abstract interpretation of the program prefix trace semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$.

– The abstraction $\alpha_h(\pi_0 \cdots \pi_n) \in \mathbb{D}$ instruments the prefix $\pi_0 \cdots \pi_n$ of a trace π in a domain $\mathbb{D}$;

– The instrumented trace $\alpha_h(\pi) \triangleq \langle \pi_0, \alpha_h(\pi_0)\rangle\langle \pi_1, \alpha_h(\pi_0\pi_1)\rangle\langle \pi_2, \alpha_h(\pi_0\pi_1\pi_2)\rangle \cdots \langle \pi_n, \alpha_h(\pi_0\pi_1 \cdots \pi_n)\rangle \cdots$ on states $\mathbb{S}^h \triangleq \mathbb{S}_{\mathbb{V}} \times \mathbb{D}$ collects this information during execution;
– The instrumented semantics is $\boldsymbol{\mathcal{S}}^h[\![\mathtt{S}]\!] \triangleq \alpha_h(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]) \in \wp(\mathbb{S}^{h^+})$ where $\alpha_h(\Pi) \triangleq \{\alpha_h(\pi) \mid \pi \in \Pi\}$ is the set of instrumented traces of the semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!] \in \wp(\mathbb{S}^+)$. It follows that $\langle \wp(\mathbb{S}^+), \subseteq\rangle \underset{\alpha_h}{\overset{\gamma_h}{\leftrightarrows}} \langle \wp(\mathbb{S}^{h^+}), \subseteq\rangle$.

We have provided the example of interval arithmetics. Another example would compute with float and collect rounding errors to guard against meaningless computations. An execution involving integers would collect their minimum and maximum values.

Moreover, the instrumented semantics must be checked by providing

– a specification S (such as an invariant, temporal logic, etc.);
– A specification abstraction $\langle \wp(\mathbb{S}^{h^+}), \subseteq\rangle \underset{\alpha_S}{\overset{\gamma_S}{\leftrightarrows}} \langle \mathbb{B}, \Leftarrow\rangle$ into Booleans checking that the specification is satisfied at runtime. In practice abstraction providing more information than a binary decision would be preferable.

The best dynamic analysis semantics $\boldsymbol{\mathcal{S}}^d[\![\mathtt{S}]\!]$ is then $\boldsymbol{\mathcal{S}}^d[\![\mathtt{S}]\!] \triangleq \alpha_S(\alpha_h(\boldsymbol{\mathcal{S}}[\![\mathtt{S}]\!]))$. An instrumented dynamic analysis can be directly derived from the instrumented semantics by considering a single execution at a time.

An example would be the specification of bounds for integer variables in a language like `Pascal`. The best dynamic analysis semantics $\boldsymbol{\mathcal{S}}^d[\![\mathtt{S}]\!]$ is implemented by runtime checks.

It might be that $\alpha_S(\alpha_h(\boldsymbol{\mathcal{S}}[\![\mathtt{S}]\!]))$ is not computable or too expensive to compute. An example is regular model checking [5] where executions are monitored by a regular expression specifying sequences of invariants (and more generally any temporal logic specification can be handled as in [5]).

In that case, what can define an approximation preorder $\mathring{\sqsubseteq}^i$ (allowing for approximate instrumentation and check) and soundness would then be $\alpha_S(\alpha_h(\boldsymbol{\mathcal{S}}[\![\mathtt{S}]\!]))$ $\mathring{\sqsubseteq}^i$ $\boldsymbol{\mathcal{S}}^d[\![\mathtt{S}]\!]$. For example, verification by regular model checking [5] would become debugging by bounding executions or ignoring some checks.

By deriving the transition system from the instrumented checking semantics $\boldsymbol{\mathcal{S}}^d[\![\mathtt{S}]\!]$, we have a formal specification of the code to be generated for the runtime analysis, thus paving the way for certified runtime analysis (similar to certified compilation [27] or certified static analysis [26]). Notice that trace abstractions are more general than simulations [28]. Notice that trace abstractions are more general than simulations [28] for such correctness proofs.

A static analysis would be derived by a further finitary abstraction of all executions defined by the instrumented semantics $\alpha_h(\boldsymbol{\mathcal{S}}[\![\mathtt{S}]\!])$ (e.g. using extrapolators and interpolators [4] or abstraction into Noetherian abstract domains).

The reduced product of the static and dynamic semantics would formalize the idea that the dynamic semantics can be simplified thanks to a preliminary static analysis. A single execution of this reduced product would certainly be more efficient since some runtime tests would have been eliminated in the reduced product. For the integer interval example, this would definitely reduce the number of runtime checks.

Acknowledgement. This work was supported in part by NSF Grant CNS-1446511. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

References

1. Bartocci, E., Falcone, Y., Francalanza, A., Reger, G.: Introduction to runtime verification. In: Lectures on Runtime Verification. Lecture Notes in Computer Science, vol. 10457, pp. 1–33. Springer (2018)
2. Brönnimann, H., Melquiond, G., Pion, S.: The design of the Boost interval arithmetic library. Theor. Comput. Sci. **351**(1), 111–118 (2006)
3. Cousot, P.: The calculational design of a generic abstract interpreter. In: Broy, M., Steinbrüggen, R. (eds.) Calculational System Design. NATO ASI Series F. IOS Press (1999)
4. Cousot, P.: Abstracting induction by extrapolation and interpolation. In: VMCAI. Lecture Notes in Computer Science, vol. 8931, pp. 19–42. Springer (2015)
5. Cousot, P.: Calculational design of a regular model checker by abstract interpretation. In: ICTAC 2019. Lecture Notes in Computer Science, vol. 11884, pp. 3–21. Springer (2019)
6. Cousot, P., Cousot, R.: Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: POPL. pp. 238–252. ACM (1977)
7. Cousot, P., Cousot, R.: Constructive versions of Tarski's fixed point theorems. Pacific Journal of Mathematics **82**(1), 43–57 (1979)
8. Cousot, P., Cousot, R.: Systematic design of program analysis frameworks. In: POPL. pp. 269–282. ACM Press (1979)
9. Cousot, P., Cousot, R.: Galois connection based abstract interpretations for strictness analysis (invited paper). In: Formal Methods in Programming and Their Applications. Lecture Notes in Computer Science, vol. 735, pp. 98–127. Springer (1993)
10. Damouche, N., Martel, M., Chapoutot, A.: Numerical program optimisation by automatic improvement of the accuracy of computations. IJIEI **6**(1/2), 115–145 (2018)
11. Delmas, D., Éric Goubault, Putot, S., Souyris, J., Tekkal, K., Védrine, F.: Towards an industrial use of FLUCTUAT on safety–critical avionics software. In: FMICS. Lecture Notes in Computer Science, vol. 5825, pp. 53–69. Springer (2009)
12. Falcone, Y., Havelund, K., Reger, G.: A tutorial on runtime verification. In: Broy, M., Peled, D., Kalus, G. (eds.) Engineering Dependable Software Systems, NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 34, pp. 141–175. IOS Press (2013)
13. Ghorbal, K., Éric Goubault, Putot, S.: The zonotope abstract domain Taylor1+. In: CAV. Lecture Notes in Computer Science, vol. 5643, pp. 627–633. Springer (2009)
14. Goldberg, D.: What every computer scientist should know about floating–point arithmetic. ACM Comput. Surv. **23**(1), 5–48 (1991)
15. Éric Goubault, Putot, S.: Static analysis of numerical algorithms. In: SAS. Lecture Notes in Computer Science, vol. 4134, pp. 18–34. Springer (2006)

16. Éric Goubault, Putot, S.: A zonotopic framework for functional abstractions. Formal Methods in System Design **47**(3), 302–360 (2015)
17. Éric Goubault, Putot, S.: Inner and outer reachability for the verification of control systems. In: HSCC. pp. 11–22. ACM (2019)
18. Éric Goubault, Putot, S., Baufreton, P., Gassino, J.: Static analysis of the accuracy in control systems: Principles and experiments. In: FMICS. Lecture Notes in Computer Science, vol. 4916, pp. 3–20. Springer (2007)
19. Éric Goubault, Putot, S., Sahlmann, L.: Inner and outer approximating flowpipes for delay differential equations. In: CAV (2). Lecture Notes in Computer Science, vol. 10982, pp. 523–541. Springer (2018)
20. Éric Goubault, Putot, S., Védrine, F.: Modular static analysis with zonotopes. In: SAS. Lecture Notes in Computer Science, vol. 7460, pp. 24–40. Springer (2012)
21. Havelund, K., Goldberg, A.: Verify your runs. In: VSTTE. Lecture Notes in Computer Science, vol. 4171, pp. 374–383. Springer (2005)
22. Havelund, K., Reger, G., Rosu, G.: Runtime verification past experiences and future projections. In: Computing and Software Science. Lecture Notes in Computer Science, vol. 10000, pp. 532–562. Springer (2019)
23. Havelund, K., Rosu, G.: Runtime verification - 17 years later. In: RV. Lecture Notes in Computer Science, vol. 11237, pp. 3–17. Springer (2018)
24. IEEE: IEEE Standard for Binary Floating–Point Arithmetic. American National Standards Institute and Institute of Electrical and Electronic Engineers, ANSI/IEEE Standard 754-1985 (1985)
25. Isaacson, E., Keller, H.B.: Analysis of Numerical Methods. Dover Books on Mathematics (1994)
26. Jourdan, J.H., Laporte, V., Blazy, S., Leroy, X., Pichardie, D.: A formally–verified C static analyzer. In: POPL. pp. 247–259. ACM (2015)
27. Leroy, X.: Formal verification of a realistic compiler. Commun. ACM **52**(7), 107–115 (2009)
28. Leroy, X.: Formally verifying a compiler: What does it mean, exactly? In: ICALP. LIPIcs, vol. 55, pp. 2:1–2:1. Schloss Dagstuhl – Leibniz–Zentrum für Informatik (2016), (Slides at https://xavierleroy.org/talks/ICALP2016.pdf)
29. Martel, M.: Rangelab: A static–analyzer to bound the accuracy of finite–precision computations. In: SYNASC. pp. 118–122. IEEE Computer Society (2011)
30. Monniaux, D.: The pitfalls of verifying floating–point computations. ACM Trans. Program. Lang. Syst. **30**(3), 12:1–12:41 (2008)
31. Moore, R.E.: Interval Analysis. Prentice Hall (1966)
32. Moore, R.E.: Methods and Applications of Interval Analysis. SIAM Studies in Applied Mathematics, SIAM (1995)
33. Moore, R.E., Kearfott, R.B., Cloud, M.J.: Introduction to Interval Analysis. Society for Industrial and Applied Mathematics (Mar 2009)
34. Mycroft, A.: The theory and practice of transforming call–by–need into call–by–value. In: Symposium on Programming. Lecture Notes in Computer Science, vol. 83, pp. 269–281. Springer (1980)
35. Older, W.J.: CLP (intervals). ACM Comput. Surv. **28**(4es), 71 (1996)
36. Older, W.J., Vellino, A.: Constraint arithmetic on real intervals. In: WCLP. pp. 175–195. MIT Press (1991)
37. Overton, M.L.: Numerical Computing with IEEE Floating Point Arithmetic – Including One Theorem, One Rule of Thumb, and One Hundred and One Exercices. SIAM (2001)

38. Truchet, C., Christie, M., Normand, J.M.: A tabu search method for interval constraints. In: CPAIOR. Lecture Notes in Computer Science, vol. 5015, pp. 372–376. Springer (2008)
39. Van Der Hoeven, J.: Ball arithmetic. In: Beckmann, A., Gaßner, C., Löwe, B. (eds.) International Workshop on Logical Approaches to Barriers in Computing and Complexity, pp. 179—208. No. 6 in Preprint–Reihe Mathematik, Ernst–Moritz–Arndt–Universität Greifswald (2010)
40. Van Der Hoeven, J., Lecerf, G.: Evaluating straight–line programs over balls. In: ARITH. pp. 142–149. IEEE Computer Society (2016)
41. Winskel, G.: A note on powerdomains and modality. In: FCT. Lecture Notes in Computer Science, vol. 158, pp. 505–514. Springer (1983)