Principles of Abstract Interpretation
MIT press
Ch. **32**, Dynamic interval analysis

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-32--interval-arithmetics-PrAbsInt.pdf

Chapter 32

Ch. **32**, Dynamic interval analysis

Interval arithmetics

- In scientific computing a real number is represented by a floating point number [IEEE, 1985].
- Because of rounding errors, the floating point computation represents an uncertain real computation.
- Ramon E. Moore [Moore, 1966; Moore, Kearfott, and Cloud, 2009] invented interval arithmetics to put bounds on rounding errors in floating point computations.
- This guarantees the uncertain real computation to be between floating point bounds

- A rare example of abstract interpretation performed at runtime!

en.wikipedia.org/wiki/Interval_arithmetic

A note on 0.1 in float

Let's see what 0.1 looks like in double-precision. First, let's write it in binary, truncated to 57 significant bits:

0.0001100110011001100110011001100110011001100110011001100110011001...

Bits 54 and beyond total to greater than half the value of bit position 53, so this rounds up to

0.0001100110011001100110011001100110011001100110011001100110011101

In decimal, this is

0.1000000000000000005551115123125782702118158340454101562 5

which is slightly greater than 0.1.

www.exploringbinary.com/why-0-point-1-does-not-exist-in-floating-point/
en.wikipedia.org/wiki/Floating-point_arithmetic
en.wikipedia.org/wiki/Single-precision_floating-point_format
en.wikipedia.org/wiki/Double-precision_floating-point_format

Principle of interval arithmetics

- Instead of computing with a floating point number representing an uncertain real x, the computation is performed with the two ends of an interval $[\underline{x}, \overline{x}])$
- $\underline{x}$ and $\overline{x}$ are floating point numbers such that $x \in [\underline{x}, \overline{x}]$.
- This is an abstraction of a trace semantics where each trace is abstracted by one or several traces:
  - The abstraction of a trace abstracts reals by float intervals along the trace.
  - Whereas a tests on a real takes one or the other alternative, tests on float intervals can take both true and false alternatives hence the several traces.

Soundness of interval arithmetics

Notations

In what follows we let $\mathbb{I}$ be either the set

- $\mathbb{Z}$ of mathematical integers,
- $[\texttt{min\_int}, \texttt{max\_int}]$ of machine integers,
- $\mathbb{Q}$ of rationals,
- $\mathbb{F}$ of floating point numbers [Goldberg, 1991; Monniaux, 2008], or
- $\mathbb{R}$ of reals.

For machine integers, we consider overflow as an error. We define

- $\min \mathbb{I} \triangleq -\infty$, $\max \mathbb{I} \triangleq \infty$, $\min \varnothing \triangleq \infty$, $\max \varnothing \triangleq -\infty$ where $-\infty = \texttt{min\_int}$ (the smallest representable integer) and $\infty = \texttt{max\_int}$ (the greatest representable integer) for machine integers (when overflow is an error)
- for modular integer arithmetics, see [Gange, Navas, Schachte, Søndergaard, and Stuckey, 2014; Müller-Olm and Seidl, 2005; Simon and King, 2007]).

Intuition for soundness of interval arithmetics

Given parameters $x \in [\underline{x}, \overline{x}]$, $y \in [\underline{y}, \overline{y}]$, ... the interval computation of a function $f \in \mathbb{I}^n \to \mathbb{I}$ must return a sound interval $[\underline{f}, \overline{f}]$ which contains all possible results for all possible values of the parameters.

$$\{f(x, y, \ldots) \mid x \in [\underline{x}, \overline{x}] \wedge y \in [\underline{y}, \overline{y}] \wedge \ldots\} \quad \subseteq \quad [\underline{f}, \overline{f}]$$

The smaller interval, the better!

Interval abstraction

Interval abstraction

- The interval abstraction abstracts a set of numerical values, possibly unbounded, by their minimum and maximal values.
- The interval abstraction is

$$\begin{array}{rcl} \alpha_i(S) & \triangleq & [\min S, \max S] \\ \gamma_i([\underline{x}, \overline{x}]) & \triangleq & \{z \in \mathbb{I} \mid \underline{x} \leqslant z \leqslant \overline{x}\} \end{array}$$

Example 1 In interval arithmetics, a real is abstracted by the pair of enclosing floats, which is also the abstraction of the set of reals between these two floats, as shown by the concretization of a float interval as the set of reals within that interval. □

- We let the abstract domain of numerical intervals be

$$\mathbb{P}^i_{\mathbb{I}} \triangleq \begin{array}{l} \{\varnothing\} \cup \{[\underline{x}, \overline{x}] \mid \underline{x} \in \mathbb{I} \wedge \underline{x} \leqslant \overline{x} \wedge \overline{x} \in \mathbb{I}\} \\ \cup \{[-\infty, \overline{x}] \mid \overline{x} \in \mathbb{I}\} \cup \{[\underline{x}, \infty] \mid \underline{x} \in \mathbb{I}\} \cup \{[-\infty, \infty]\} \end{array}$$

  where the empty interval $\bot^i = \varnothing$ can be encoded by any $[\underline{x}, \overline{x}]$ with $\overline{x} < \underline{x}$ (*e.g.* normalized to $[\infty, -\infty]$).
- The intervals $[-\infty, -\infty] \notin \mathbb{P}^i_{\mathbb{I}}$ and $[\infty, \infty] \notin \mathbb{P}^i_{\mathbb{I}}$ are excluded.
- For machine integers $\mathbb{I} = [\texttt{min\_int}, \texttt{max\_int}]$ where $-\infty = \texttt{min\_int}$ and $\infty = \texttt{max\_int}$, we have $\mathbb{P}^i_{\mathbb{I}} \triangleq \{\varnothing\} \cup \{[\underline{x}, \overline{x}] \mid \texttt{min\_int} \leqslant \underline{x} \leqslant \overline{x} \leqslant \texttt{max\_int}\}$.
- The partial order $\sqsubseteq^i$ on $\mathbb{P}^i_{\mathbb{I}}$ is interval inclusion $\bot^i \sqsubseteq^i \bot^i \sqsubseteq^i [\underline{x}, \overline{x}] \sqsubseteq^i [\underline{y}, \overline{y}]$ if and only if $\underline{y} \leqslant \underline{x} \leqslant \overline{x} \leqslant \overline{y}$.
- We have the Galois connection

$$\langle \wp(\mathbb{I}), \subseteq \rangle \underset{\alpha_i}{\overset{\gamma_i}{\leftrightarrows}} \langle \mathbb{P}^i_{\mathbb{I}}, \sqsubseteq^i \rangle \tag{32.3}$$

- The soundness condition becomes

$$\alpha_i(\{f(x, y, \ldots) \mid x \in \gamma_i([\underline{x}, \overline{x}]) \wedge y \in \gamma_i([\underline{y}, \overline{y}]) \wedge \ldots\}) \quad \sqsubseteq^i \quad [\underline{f}, \overline{f}].$$

Interval arithmetics

Constants

- If the program contains a constant c, its interval is $[c, c]$.
- However, the compilation may introduce an error *i.e.* overflow with integers or rounding error for a float that must be taken into account.
- For example, the decimal 0.1 is $0.000(1100)^{\infty}$ in binary so has no exact binary representation on finitely many bits.

Addition and substraction

$$
\begin{aligned}
[\underline{x}, \overline{x}] \oplus^i \varnothing &= \varnothing \oplus^i [\underline{x}, \overline{x}] = [\underline{x}, \overline{x}] \ominus^i \varnothing = \varnothing \ominus^i [\underline{x}, \overline{x}] = \varnothing \\
[\underline{x}, \overline{x}] \oplus^i [\underline{y}, \overline{y}] &= [\underline{x} + \underline{y}, \overline{x} + \overline{y}] \\
[\underline{x}, \overline{x}] \ominus^i [\underline{y}, \overline{y}] &= [\underline{x} - \overline{y}, \overline{x} - \underline{y}] \\
\ominus^i [\underline{x}, \overline{x}] &= [-\overline{x}, -\underline{x}]
\end{aligned}
$$

- We assume that $-\infty + -\infty = -\infty$, $-\infty + z = -\infty$, $\infty + z = \infty$, and $\infty + \infty = \infty$ for any $z \in \mathbb{I}$.
- For example, $[10, \infty] \ominus^i [-\infty, 5] = [10 - 5, \infty - (-\infty)] = [5, \infty]$.
- For floating point numbers, the lower bound is rounded towards $-\infty$ and the upper bound towards $+\infty$.
- This implies that the computed value is always included in the concretization of the interval value.

Proof The proof is by calculational design. The case of $\varnothing$ is trivial. Otherwise

$$\begin{aligned}
&\alpha_i(\{x+y \mid x \in \gamma_i([\underline{x},\overline{x}]) \wedge y \in \gamma_i([\underline{y},\overline{y}])\}) \\
\triangleq\ &\text{let } S = \{x+y \mid \underline{x} \leqslant x \leqslant \overline{x} \wedge \underline{y} \leqslant y \leqslant \overline{y}\} \text{ in } [\min S, \max S] && \text{(def. } \gamma_i \text{ and } \gamma_i\text{)} \\
=\ &\text{let } S = \{x+y \mid \underline{x}+\underline{y} \leqslant x+y \leqslant \overline{x}+\overline{y}\} \text{ in } [\min S, \max S] \\
& && \text{(The sum is minimal for minimal parameters, same for maximal)} \\
=\ &[\underline{x}+\underline{y}, \overline{x}+\overline{y}]
\end{aligned}$$

(by considering all cases when $\underline{x}$, $\overline{x}$, $\underline{y}$, and $\overline{y}$ are infinite or integer bounds.

- When $\underline{x} \leqslant \overline{x}$ and $\underline{y} \leqslant \overline{y}$ belong to $\mathbb{I}$, we have $\{x+y \mid \underline{x} \leqslant x \leqslant \overline{x} \wedge \underline{y} \leqslant y \leqslant \overline{y}\} = \{x+y \mid \underline{x}+\underline{y} \leqslant x+y \leqslant \overline{x}+\overline{y}\}$ since $(\underline{x} \leqslant x \leqslant \overline{x} \wedge \underline{y} \leqslant y \leqslant \overline{y}) \Rightarrow (\underline{x}+\underline{y} \leqslant x+y \leqslant \overline{x}+\overline{y})$ and conversely, $(\underline{x}+\underline{y} \leqslant x+y \leqslant \overline{x}+\overline{y}) \Rightarrow (\exists x', y' \in \mathbb{I} \,.\, \underline{x} \leqslant x' \leqslant \overline{x} \wedge \underline{y} \leqslant y' \leqslant \overline{y} \wedge x'+y' = x+y)$. It follows that $[\min S, \max S] = [\underline{x}+\underline{y}, \overline{x}+\overline{y}]$;

- When $\underline{x} = \underline{y} = -\infty$ and $\overline{x} = \overline{y} = \infty$, we have $\{x + y \mid \underline{x} + \underline{y} \leqslant x + y \leqslant \overline{x} + \overline{y}\} = \{x + y \mid x \in \mathbb{I} \wedge y \in \mathbb{I}\} = \mathbb{I}$ with $[\min \mathbb{I}, \max \mathbb{I}] = [-\infty, \infty]$; $= [-\infty + -\infty, \infty + \infty]$;
- *etc.* ʃ

$= [\underline{x}, \overline{x}] \oplus^i [\underline{y}, \overline{y}]$ ʅby defining $[\underline{x}, \overline{x}] \oplus^i [\underline{y}, \overline{y}] = [\underline{x} + \underline{y}, \overline{x} + \overline{y}]$ʃ

The proof for the binary $\ominus^i$ is similar and for the unary minus $\ominus^i[\underline{y}, \overline{y}] = [0, 0] \ominus^i [\underline{y}, \overline{y}]$.□

Multiplication

$$
\begin{array}{rcl}
[\underline{x}, \overline{x}] \otimes^i \varnothing & = & \varnothing \otimes^i [\underline{x}, \overline{x}] \quad = \quad \varnothing \\
[\underline{x}, \overline{x}] \otimes^i [\underline{y}, \overline{y}] & = & [\min(\underline{x}\,\underline{y}, \underline{x}\,\overline{y}, \overline{x}\,\underline{y}, \overline{x}\,\overline{y}), \max(\underline{x}\,\underline{y}, \underline{x}\,\overline{y}, \overline{x}\,\underline{y}, \overline{x}\,\overline{y})]
\end{array}
$$

which reduces to $[\underline{x}\,\underline{y}, \overline{x}\,\overline{y}]$ when the lower bounds $\underline{x}$ and $\underline{y}$ are greater that zero.

Reciprocal and division

- The interval reciprocal is

$$
\begin{array}{lcll}
[1,1] \oslash^i [\underline{x}, \overline{x}] & \triangleq & [1/\overline{x}, 1/\underline{x}] & \text{when } \overline{x} < 0 \text{ or } 0 < \underline{x} \\
[1,1] \oslash^i [\underline{x}, \overline{x}] & \triangleq & [-\infty, \infty] & \text{otherwise } (\tfrac{1}{0} = \pm\infty)
\end{array}
$$

- The division can then be handled as $[\underline{x}, \overline{x}] \oslash^i [\underline{y}, \overline{y}] = [\underline{x}, \overline{x}] \otimes ([1,1] \oslash^i [\underline{y}, \overline{y}])$.
- A more precise treatment of interval division is proposed in [Hickey, Ju, and van Emden, 2001, Sect. 4.7].

Algebraic properties

- The interval operations have some of the usual algebraic properties of arithmetic operations

$$
\begin{array}{rcll}
(x \oplus^i y) \oplus^i z & = & x \oplus^i (y \oplus^i kz) & \text{associativity} \\
(x \ominus^i y) \ominus^i z & = & x \ominus^i (y \ominus^i z) & \\
x \oplus^i y & = & y \oplus^i x & \text{commutativity} \\
x \otimes y & = & y \otimes^i x & \\
x \oplus^i [0,0] & = & x & \text{neutral element} \\
x \otimes^i [1,1] & = & x &
\end{array}
$$

- However distributivity does not hold. We have

$$x \otimes^i (y \oplus^i z) \quad \sqsubseteq^i \quad (x \otimes^i y) \oplus^i (x \otimes^i z) \qquad \text{subdistributivity}$$

Arithmetic expressions

- The interval semantics $\mathscr{A}^i[\![\mathtt{A}]\!]$ of an arithmetic expression $\mathtt{A}$ is similar to the cartesian evaluation of arithmetic expressions (28.13) which is the semantics of expressions (3.4) on $\mathbb{I}$ where values in $\mathbb{I}$ are replaced by intervals in $\mathbb{P}^i$ abstracting $\wp(\mathbb{I})$.
- The interval semantics $\mathscr{A}^i[\![\mathtt{A}]\!]$ does not preverve lubs in general.
- For example $\forall n \in \mathbb{I} \,.\, \mathscr{A}^i[\![\mathtt{x} - \mathtt{x}]\!]\rho[\mathtt{x} \leftarrow [n,n]] = [0,0]$ whereas for $\rho[\mathtt{x} \leftarrow [-\infty,\infty]] = \dot{\bigsqcup}^i_{n\in\mathbb{I}} \rho[\mathtt{x} \leftarrow [n,n]]$, $\mathscr{A}^i[\![\mathtt{x} - \mathtt{x}]\!]\rho[\mathtt{x} \leftarrow [-\infty,\infty]] = [-\infty,\infty]$.
- More generally, relations between variables are lost which is the cause of imprecision.
- This can be improved by coupling interval arithmetics with a relational analysis (through a reduced product of Chapter **36**), see *e.g.* [Darulova and Kuncak, 2017; de Figueiredo and Stolfi, 2004].

Conditions

- Although when computing with $\mathbb{I}$ only one branch of a conditional will be taken, interval computation with $\mathbb{P}^i_{\mathbb{I}}$ may have to take both.
- This gives, in the worst-case, an exponential number of cases to consider.
- In most interval arithmetic libraries, this case raises an exception that stops execution, which is a further coarse abstraction of the abstract semantics presented here *e.g.*
  `www.boost.org/doc/libs/1_74_0/libs/numeric/interval/doc/interval.htm`, `www.boost.org/doc/libs/1_74_0/libs/numeric/interval/doc/comparisons.htm`.

Conditions (cont'd)

- The boolean comparison operators $x \circledcirc y$ take two intervals for x and y and return two intervals for x and y such that the comparison may hold (and cannot hold outside these intervals).

$$
\begin{array}{lcll}
[\underline{x}, \overline{x}] \ominus^i [\underline{y}, \overline{y}] & \triangleq & \langle \varnothing, \varnothing \rangle & \text{if } \overline{x} < \underline{y} \text{ or } \overline{y} < \underline{x} \\
& \triangleq & \langle [\max(\underline{x}, \underline{y}), \min(\overline{x}, \overline{y})], [\max(\underline{x}, \underline{y}), \min(\overline{x}, \overline{y})] \rangle & \text{otherwise} \\
[\underline{x}, \overline{x}] \oslash^i [\underline{y}, \overline{y}] & \triangleq & \langle \varnothing, \varnothing \rangle & \text{if } \underline{x} \geqslant \overline{y} \\
& \triangleq & \langle [\underline{x}, \min(\overline{x}, \overline{y})], [\max(\underline{x}, \underline{y}), \overline{y}] \rangle & \text{otherwise, } \mathbb{I} \neq \mathbb{Z} \\
& \triangleq & \langle [\underline{x}, \min(\overline{x}, \overline{y} - 1)], [\max(\underline{x} + 1, \underline{y}), \overline{y}] \rangle & \text{otherwise, } \mathbb{I} = \mathbb{Z}
\end{array}
$$

Backward interval arithmetics

Backward interval arithmetics

- For interval static analysis in Chapter **33**, we need the following backward interval arithmetics operators.
- $\ominus^{\overset{i}{\cdot}_1}\,[a,b]\langle[\underline{x},\overline{x}],\ [\underline{y},\overline{y}]\rangle \triangleq \langle[\max(\underline{x},a+\underline{y}),\min(\overline{x},b+\overline{y})],\ [\max(\underline{y},\underline{x}-b),\min(\overline{y},\overline{x}-a)]\rangle$;
- $\circledcirc^{\overset{i}{\cdot}_1}\,\langle[\underline{x},\overline{x}],\ [\underline{y},\overline{y}]\rangle \triangleq \langle[\underline{x},\min(\overline{x},\overline{y}-1)],\ [\max(\underline{y},\underline{x}+1),\overline{y}]\rangle$;
- $\overline{\circledcirc}^{\overset{i}{\cdot}_1}\,\langle[\underline{x},\overline{x}],\ [\underline{y},\overline{y}]\rangle \triangleq \langle[\max(\underline{x},\underline{y}),\overline{x}],\ [\underline{y},\min(\overline{x},\overline{y})]\rangle$.

- For example $\ominus^{\overset{i}{\cdot}_1}\,[0,0]\langle[0,1],\ [-1,0]\rangle = \langle[0,0],\ [0,0]\rangle$ since for the difference of $a \in [0,1]$ and $b \in [-1,0]$ to be 0, we must have $a = b = 0$.
- $\ominus^{\overset{i}{\cdot}_1}\,[0,0]\langle[1,\infty],\ [-\infty,0]\rangle = \langle[1,0],\ [1,0]\rangle = \langle\varnothing,\ \varnothing\rangle$ since the difference of a strictly positive number and a negative number cannot be null.

Semantics of real and float arithmetic expressions

Syntax and real or float semantics of arithmetic expressions

- Syntax

$$\mathtt{A} \in \mathcal{A} ::= \mathtt{1} \mid \mathtt{0.1} \mid \mathtt{x} \mid \mathtt{A}_1 - \mathtt{A}_2 \qquad \text{arithmetic expressions}$$

- $\mathbb{V}$ was $\mathbb{Z}$ is now either the $\mathbb{R}$ of reals (at least mathematically) or the set $\mathbb{F}$ of floats (and later the set $\mathbb{P}^i_{\mathbb{F}}$ of all float intervals).
- We write $\mathcal{S}^*_{\mathbb{V}}[\![\mathtt{S}]\!]$ to make explicit which set of values $\mathbb{V}$ is considered in computations.
- Value of an arithmetic expression $\mathtt{A}$ in environment $\rho \in \mathbb{E}\mathrm{v}_{\mathbb{V}} \triangleq \mathcal{V} \to \mathbb{V}$ is now $\mathcal{A}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho \in \mathbb{V}$ defined as

$$\begin{array}{llll} \mathcal{A}_{\mathbb{V}}[\![\mathtt{1}]\!]\rho & \triangleq & 1 & \mathcal{A}_{\mathbb{V}}[\![\mathtt{0.1}]\!]\rho \triangleq 0.1_{\mathbb{V}} \\ \mathcal{A}_{\mathbb{V}}[\![\mathtt{x}]\!]\rho & \triangleq & \rho(\mathtt{x}) & \mathcal{A}_{\mathbb{V}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\rho \triangleq \mathcal{A}_{\mathbb{V}}[\![\mathtt{A}_1]\!]\rho -_{\mathbb{V}} \mathcal{A}_{\mathbb{V}}[\![\mathtt{A}_2]\!]\rho \end{array} \tag{32.11}$$

- For example $-_{\mathbb{F}}$ is the difference found on IEEE-754 machines and must take rounding mode (and the machine specificities [Monniaux, 2008]) into account.

Float notations

- $\overleftarrow{\lceil} x$ (which can be $-\infty$) is the largest float smaller than or equal to $x \in \mathbb{R}$ (or $\overleftarrow{\lceil} x = x$ for $x \in \mathbb{F}$)
- $x \overrightarrow{\rceil}$ (which can be $+\infty$) is the smallest float greater than or equal to $x \in \mathbb{R}$ (or $x \overrightarrow{\rceil} = x$ for $x \in \mathbb{F}$).
- $\overleftarrow{\lfloor} x$ is the largest floating-point number strictly less than $x \in \mathbb{F}$ (which can be $-\infty$)
- $x \overrightarrow{\lfloor}$ is the smallest floating-point number strictly larger than $x \in \mathbb{F}$ (which can be $+\infty$).
- We assume

$$\begin{array}{rcll} \overleftarrow{\lceil} x -_{\mathbb{F}} y \overrightarrow{\rceil} & \leqslant & \overleftarrow{\lceil} (x -_{\mathbb{V}} y) & (\mathbb{V} \text{ is } \mathbb{R} \text{ or } \mathbb{F}) \quad (32.12) \\ x \overrightarrow{\rceil} -_{\mathbb{F}} \overleftarrow{\lceil} y & \geqslant & (x -_{\mathbb{V}} y) \overrightarrow{\rceil} & \\ (\mathsf{x} \in [\underline{x}, \overline{x}] \wedge \mathsf{y} \in [\underline{y}, \overline{y}] \wedge \mathsf{x} < \mathsf{y}) & \Rightarrow & (\mathsf{x} \in [\underline{x}, \min(\overline{x}, \overline{y})] \wedge \mathsf{y} \in [\max(\underline{x}, \underline{y}), \overline{y}]) & (32.13) \end{array}$$

Incorrect machine implementations

- Some machine implementations of IEEE-754 floating point arithmetics [IEEE, 1985] are incorrect [Goldberg, 1991; Monniaux, 2008].
- For example [Monniaux, 2008, Sect. 6.1.2], we could have

$$(x \in [\underline{x}, \overline{x}] \wedge y \in [\underline{y}, \overline{y}] \wedge x < y) \quad \Rightarrow \quad (x \in [\underline{x}, \min(\overline{x}, \overline{y}\lceil^{\rightarrow})] \wedge y \in [\max(\lceil^{\leftarrow}\underline{x}, \underline{y}), \overline{y}]) \qquad (32.13.bis)$$

en.wikipedia.org/wiki/Pentium_FDIV_bug

Float interval abstraction of arithmetic expressions

Float interval abstraction

$$
\begin{array}{rcll}
\alpha^i_{\mathbb{F}}(x) & \triangleq & [\overleftarrow{\P} x, x \overrightarrow{\P}] & \text{real/float abstraction by float interval} \quad (32.14) \\
\gamma^i_{\mathbb{F}}([\underline{x}, \overline{x}]) & \triangleq & \{x \in \mathbb{R} \mid \underline{x} \leqslant x \leqslant \overline{x}\} & \\
\dot{\alpha}^i_{\mathbb{F}}(\rho) & \triangleq & \mathtt{x} \in \mathbb{V} \mapsto \dot{\alpha}^i_{\mathbb{F}}(\rho(\mathtt{x})) & \text{environment abstraction} \\
\dot{\gamma}^i_{\mathbb{F}}(\overline{\rho}) & \triangleq & \{\rho \in \mathbb{V} \to \mathbb{R} \mid \forall \mathtt{x} \in \mathbb{V} \,.\, \rho(\mathtt{x}) \in \gamma^i_{\mathbb{F}}(\overline{\rho}(\mathtt{x}))\} &
\end{array}
$$

The Galois connection (32.3) for float intervals is extended pointwise $\rho \mathbin{\dot{\sqsubseteq}^i} \rho' \triangleq \forall \mathtt{x} \in \mathbb{V} \,.\, \rho(\mathtt{x}) \sqsubseteq^i \rho'(\mathtt{x})$ to interval environments (mapping variables to their interval of values).

$$\langle \wp(\mathbb{R}), \subseteq \rangle \underset{\alpha^i_{\mathbb{F}}}{\overset{\gamma^i_{\mathbb{F}}}{\leftrightarrows}} \langle \mathbb{P}^i_{\mathbb{F}}, \sqsubseteq^i \rangle \quad (32.3) \qquad \langle \wp(\mathbb{V} \to \mathbb{R}), \subseteq \rangle \underset{\dot{\alpha}^i_{\mathbb{F}}}{\overset{\dot{\gamma}^i_{\mathbb{F}}}{\leftrightarrows}} \langle \mathbb{V} \to \mathbb{P}^i_{\mathbb{F}}, \mathbin{\dot{\sqsubseteq}^i} \rangle \quad (32.15)$$

Float interval abstraction of an arithmetic expression

- Let $\mathbb{V}$ be $\mathbb{R}$ or $\mathbb{F}$.

$$\begin{array}{rcll} \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{1}]\!]\rho & \triangleq & 1_{\mathbb{F}} & \text{where } 1_{\mathbb{F}} = [1,1] \text{ and } 1 \in \mathbb{F} \\ \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{0.1}]\!]\rho & \triangleq & 0.1_{\mathbb{F}} & \text{where } 0.1_{\mathbb{F}} \triangleq [\overleftarrow{\P} 0.1_{\mathbb{V}}, 0.1_{\mathbb{V}} \overrightarrow{\P}] \\ \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{x}]\!]\rho & \triangleq & \rho(\mathtt{x}) & \\ \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\rho & \triangleq & \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{A}_1]\!]\rho \ominus^i_{\mathbb{F}} \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{A}_2]\!]\rho & \text{where } [\underline{x}, \overline{x}] \ominus^i_{\mathbb{F}} [\underline{y}, \overline{y}] \triangleq [\underline{x} -_{\mathbb{F}} \overline{y}, \overline{x} -_{\mathbb{F}} \underline{y}] \end{array} \tag{32.17}$$

  is such that

$$\alpha^i_{\mathbb{F}}(\mathscr{A}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho) \quad \sqsubseteq^i \quad \mathscr{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\dot{\alpha}^i_{\mathbb{F}}(\rho). \tag{32.16}$$

- $\mathscr{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]$ is $\dot{\sqsubseteq}^i$-increasing.

About division

- If we had a division, we would have to handle NaN (Not a Number) interpreted as a value that is undefined or unrepresentable.
- A simple way is to stop execution, by choosing $\mathscr{A}^i_{\mathbb{F}}[\![\texttt{1 / 0}]\!]\overline{\rho} \triangleq \varnothing$.
- 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 choose the first alternative, which is simpler.

en.wikipedia.org/wiki/IEEE_754

Float interval abstraction of boolean expressions

Float interval abstraction of a boolean expression

- 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 $\mathbb{V} = \mathbb{P}^i_{\mathbb{F}}$.
- Moreover in case of uncertainty (*e.g.* $<$ is handled as $\leqslant$) the two part may overlap. Therefore we assume that the abstract interpretation $\mathscr{B}\!\!\mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]$ of a boolean expression $\mathtt{B}$ is defined such that

$$\begin{array}{l}
\text{let } \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \rangle = \mathscr{B}\!\!\mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!](\dot{\alpha}^i_{\mathbb{F}}(\rho)) \text{ in} \qquad (32.18)\\
\quad \dot{\alpha}^i_{\mathbb{F}}(\rho) \;\dot{\sqsubseteq}^i\; \overline{\rho}_{\mathtt{tt}} \qquad \text{if} \quad \mathscr{B}\!\!\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{tt}\\
\quad \dot{\alpha}^i_{\mathbb{F}}(\rho) \;\dot{\sqsubseteq}^i\; \overline{\rho}_{\mathtt{ff}} \qquad \text{if} \quad \mathscr{B}\!\!\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\rho = \mathtt{ff}\\
\text{and } (\langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \rangle = \mathscr{B}\!\!\mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\overline{\rho}) \Rightarrow (\overline{\rho}_{\mathtt{tt}} \;\dot{\sqsubseteq}^i\; \overline{\rho} \wedge \overline{\rho}_{\mathtt{ff}} \;\dot{\sqsubseteq}^i\; \overline{\rho})\\
\text{and } \mathscr{B}\!\!\mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!] \text{is increasing}
\end{array}$$

- 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 change values of variables.

Interval boolean expressions have side-effects, Section **32.5.5**

- The evaluation of integer, float and real boolean expressions has no side-effect.
- Formally,

$$\varrho(\pi^\ell) \quad = \quad \varrho(\pi^\ell \xrightarrow{\texttt{B}/\neg(\texttt{B})} \ell')$$

  as shown by the def. (6.6) of ϱ.
- This is no longer the case with interval arithmetics!
- For example, assume that $\varrho(\pi^\ell)\texttt{x} = [-0.1, 0.1]$. Then $\varrho(\pi^\ell \xrightarrow{\texttt{(x > 0)}} \ell') = [0, 0.1]$ while $\varrho(\pi^\ell \xrightarrow{\neg\texttt{(x > 0)}} \ell') = [-0.1, 0]$.
- `>` is handled as `>=` since intervals are closed
- the interval of value of `x` is changed by the test, which has a side-effect.

Interval boolean expressions have side-effects, Section **32.5.5** (cont'd)

- We take side effects into account by
  - recording the value of variables after the test in the boolean actions which become $\mathtt{B} = \rho$ and $\neg(\mathtt{B}) = \rho$ where $\rho \in \mathbb{E}\mathbb{v}$ is the environment passing the test;
  - changing the computation (6.6) of the value of variable $\mathtt{x} \in \mathbb{V}$ at the end of a trace π as follows

$$
\begin{array}{rcll}
\boldsymbol{\varrho}(\pi\ell \xrightarrow{\mathtt{x} = \mathtt{A} = \nu} \ell')\mathtt{x} & \triangleq & \nu & (32.19)\\
\boldsymbol{\varrho}(\pi\ell \xrightarrow{\mathtt{B} = \rho} \ell')\mathtt{x} & \triangleq & \rho(\mathtt{x}) & \\
\boldsymbol{\varrho}(\pi\ell \xrightarrow{\neg(\mathtt{B}) = \rho} \ell')\mathtt{x} & \triangleq & \rho(\mathtt{x}) & \\
\boldsymbol{\varrho}(\pi\ell \xrightarrow{\cdots} \ell')\mathtt{x} & \triangleq & \boldsymbol{\varrho}(\pi\ell)\mathtt{x} & \text{otherwise}\\
\boldsymbol{\varrho}(\ell)\mathtt{x} & \triangleq & 0 &
\end{array}
$$

Interval boolean expressions have side-effects, Section **32.5.5** (cont'd)

- In the prefix and maximal trace semantics for float intervals, we change the traces $\pi \xrightarrow{\mathtt{B}/\neg(\mathtt{B})} \pi'$ to
  - $\pi \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \pi'$
  - $\pi \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \pi'$

  where $\langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \rangle = \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\, \varrho(\pi)$

Float interval abstraction of execution traces

Abstraction of real traces by float interval traces

- We write $\mathbb{T}^{+}_{\mathbb{V}}$, $\mathbb{T}^{\infty}_{\mathbb{V}}$, and $\mathbb{T}^{+\infty}_{\mathbb{V}}$ for $\mathbb{V} = \mathbb{R}$, $\mathbb{V} = \mathbb{F}$, and $\mathbb{V} = \mathbb{P}^{i}_{\mathbb{F}}$.
- Given a real trace semantics *i.e.* a set $\Pi \in \wp(\mathbb{T}^{+\infty}_{\mathbb{R}})$, we define a float interval trace semantics $\mathring{\alpha}^{i}_{\mathbb{F}}(\Pi) \in \wp(\mathbb{T}^{+\infty}_{\mathbb{P}^{i}_{\mathbb{F}}})$ by abstracting the real $x \in \mathbb{R}$ values by an interval $\alpha^{i}_{\mathbb{F}}(x) = [\overleftarrow{\P} x, x \overrightarrow{\P}]$.
- 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 $x \in [\overleftarrow{\P} x, x \overrightarrow{\P}]$.

Abstraction of real traces by float interval traces (cont'd)

- Formally, the abstraction of a trace abstracts real values computed along the trace into a float interval.

$$
\begin{array}{rcll}
\bar{\alpha}^i_{\mathbb{F}}(\mathtt{x = A} = v) & \triangleq & \mathtt{x = A} = \alpha^i_{\mathbb{F}}(v) & \text{action abstraction} \qquad (32.20)\\
\bar{\alpha}^i_{\mathbb{F}}(\mathtt{B} = \rho) & \triangleq & \mathtt{B} = \overline{\rho}_{\mathtt{tt}} & \text{if } \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \rangle = \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!](\dot{\alpha}^i_{\mathbb{F}}(\rho))\\
\bar{\alpha}^i_{\mathbb{F}}(\neg(\mathtt{B}) = \rho) & \triangleq & \neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}} & \text{if } \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \rangle = \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!](\dot{\alpha}^i_{\mathbb{F}}(\rho))\\
\bar{\alpha}^i_{\mathbb{F}}(\mathtt{a}) & \triangleq & \mathtt{a} & \text{otherwise}\\
\bar{\gamma}^i_{\mathbb{F}}(\mathtt{x = A} = \overline{v}) & \triangleq & \{\mathtt{x = A} = v \mid v \in \gamma^i_{\mathbb{F}}(\overline{v})\} & \\
\bar{\gamma}^i_{\mathbb{F}}(\mathtt{B} = \overline{\rho}) & \triangleq & \{\mathtt{B} = \rho \mid \rho \in \dot{\gamma}^i_{\mathbb{F}}(\overline{\rho})\} & \\
\bar{\gamma}^i_{\mathbb{F}}(\neg(\mathtt{B}) = \overline{\rho}) & \triangleq & \{\neg(\mathtt{B}) = \rho \mid \rho \in \dot{\gamma}^i_{\mathbb{F}}(\overline{\rho})\} & \\
\bar{\gamma}^i_{\mathbb{F}}(\mathtt{a}) & \triangleq & \{\mathtt{a}\} & \text{otherwise}
\end{array}
$$

Abstraction of real traces by float interval traces (cont'd)

- [In]finite trace abstraction:

$$\vec{\alpha}^i_{\mathbb{F}}(\ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \dots \ell_n \xrightarrow{\mathtt{a}_n} \ell_{n+1} \dots) \triangleq (\ell_1 \xrightarrow{\vec{\alpha}^i_{\mathbb{F}}(\mathtt{a}_1)} \ell_2 \dots \ell_n \xrightarrow{\vec{\alpha}^i_{\mathbb{F}}(\mathtt{a}_n)} \ell_{n+1} \dots) \tag{32.21}$$

$$\vec{\gamma}^i_{\mathbb{F}}(\overline{\pi}) \triangleq \text{let } \ell_1 \xrightarrow{\overline{\mathtt{a}}_1} \ell_2 \dots \ell_n \xrightarrow{\overline{\mathtt{a}}_n} \ell_{n+1} \dots = \overline{\pi} \text{ in}$$
$$\{\pi \mid |\pi| = |\overline{\pi}| \wedge \pi = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \dots \ell_n \xrightarrow{\mathtt{a}_n} \ell_{n+1} \dots \wedge$$
$$\forall i = 1, \dots, n, \dots . \ \mathtt{a}_i \in \vec{\gamma}^i_{\mathbb{F}}(\overline{\mathtt{a}}_i)\}$$

such that $\dot{\alpha}^i_{\mathbb{F}}(\varrho(\pi)) \dot{\sqsubseteq}^i \varrho(\vec{\alpha}^i_{\mathbb{F}}(\pi))$ (by def. (32.19) of ϱ) (32.22)

- This trace abstraction is extended componentwise to pairs $\langle \pi, \pi' \rangle$ of an initialization trace π and a continuation trace π'.

$$\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi, \pi' \rangle) \triangleq \langle \vec{\alpha}^i_{\mathbb{F}}(\pi), \vec{\alpha}^i_{\mathbb{F}}(\pi') \rangle \quad \text{pairwise abstraction} \tag{32.23}$$
$$\ddot{\gamma}^i_{\mathbb{F}}(\langle \overline{\pi}, \overline{\pi}' \rangle) \triangleq \{\langle \pi, \pi' \rangle \mid \pi \in \vec{\gamma}^i_{\mathbb{F}}(\overline{\pi}) \wedge \pi' \in \vec{\gamma}^i_{\mathbb{F}}(\overline{\pi}')\}$$

Abstraction of real traces by float interval traces (cont'd)

- This pair of traces abstraction is extended elementwise to trace semantics *i.e.* sets of pairs of traces (see Section **6.10**)

$$\mathring{\alpha}^i_{\mathbb{F}}(\Pi) \triangleq \{\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi, \pi' \rangle) \mid \langle \pi, \pi' \rangle \in \Pi\} \qquad \text{set of traces abstraction} \quad (32.24)$$
$$\mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}) \triangleq \{\langle \pi, \pi' \rangle \mid \ddot{\alpha}^i_{\mathbb{F}}(\langle \pi, \pi' \rangle) \in \overline{\Pi}\} = \bigcup \{\ddot{\gamma}^i_{\mathbb{F}}(\langle \overline{\pi}, \overline{\pi}' \rangle) \mid \langle \overline{\pi}, \overline{\pi}' \rangle \in \overline{\Pi}\}$$

so that, by Exercise 11.6, we have the Galois connection

$$\langle \wp(\mathbb{T}^{+\infty}_{\mathbb{V}}), \subseteq \rangle \underset{\mathring{\alpha}^i_{\mathbb{F}}}{\overset{\mathring{\gamma}^i_{\mathbb{F}}}{\leftrightarrows}} \langle \wp(\mathbb{T}^{+\infty}_{\mathbb{P}^i_{\mathbb{F}}}), \subseteq \rangle \qquad (32.25)$$

- Because the floats are a subset of the reals, we can use $\mathring{\alpha}^i_{\mathbb{F}}$ to abstract sets of both real and float traces (*i.e.* whether $\mathbb{V}$ be $\mathbb{R}$ or $\mathbb{F}$).

Sound over-approximation in the concrete

- Let $\Pi = \{\langle \ell_1,\ \ell_1 \xrightarrow{\texttt{x = 1} = 1_{\mathbb{R}}} \ell_2 \xrightarrow{\texttt{x = x + 0.1} = 1.1_{\mathbb{R}}} \ell_3 \rangle\}$ be a semantics on $\mathbb{R}$.
- Let $\overline{\Pi}_1 = \alpha^i_{\mathbb{F}}(\Pi) = \{\langle \ell_1,\ \ell_1 \xrightarrow{\texttt{x = 1} = [0.99, 1.01]} \ell_2 \xrightarrow{\texttt{x = x + 0.1} = [1.09, 1.11]} \ell_3 \rangle\}$ (where each trace π of Π is over-approximated by a trace $\vec{\alpha}^i_{\mathbb{F}}(\pi)$ of $\overline{\Pi}_1$ with a ± 0.01 rounding interval.)
- We have $\Pi \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}_1)$ so $\overline{\Pi}_1$ is a sound over-approximation of Π.
- But $\overline{\Pi}_2 = \{\langle \ell_1,\ \ell_1 \xrightarrow{\texttt{x = 1} = [0.99, 1.01]} \ell_2 \xrightarrow{\texttt{x = x + 0.1} = [0, 1.1]} \ell_3 \rangle, \langle \ell_1,\ \ell_1 \xrightarrow{\texttt{x = 1} = [0.99, 1.01]} \ell_2 \xrightarrow{\texttt{x = x + 0.1} = [1.1, 2]} \ell_3 \rangle\}$ is also a sound over-approximation of Π since $\Pi \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}_2)$.
- Although $\overline{\Pi}_1 \in \wp(\mathbb{T}^{+\infty}_{\mathbb{P}^i_{\mathbb{F}}})$ is more precise than $\overline{\Pi}_2 \in \wp(\mathbb{T}^{+\infty}_{\mathbb{P}^i_{\mathbb{F}}})$, they are not comparable as abstract elements of $\langle \wp(\mathbb{T}^{+\infty}_{\mathbb{P}^i_{\mathbb{F}}}), \subseteq \rangle$ in (32.25).
- The intuition that $\overline{\Pi}_1$ is more precise than $\overline{\Pi}_2$ is by comparison in the concrete that is $\mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}_1) \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}_2)$.

Concrete and abstract soundness of the float interval abstraction of execution traces

Sound over-approximation in the concrete (cont'd)

- 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.

$$\begin{aligned}\overline{\Pi} \mathring{\sqsubseteq}^i \overline{\Pi}' &\triangleq \mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}) \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\overline{\Pi}') \\ &= \forall \langle \overline{\pi}_0, \overline{\pi}_1 \rangle \in \overline{\Pi} \,.\, \forall \langle \pi_0, \pi_1 \rangle \in \ddot{\gamma}^i_{\mathbb{F}}(\langle \overline{\pi}_0, \overline{\pi}_1 \rangle) \,.\\ &\qquad \exists \langle \overline{\pi}'_0, \overline{\pi}'_1 \rangle \in \overline{\Pi}' \,.\, \langle \pi_0, \pi_1 \rangle \in \ddot{\gamma}^i_{\mathbb{F}}(\langle \overline{\pi}'_0, \overline{\pi}'_1 \rangle\end{aligned} \tag{32.26}$$

- Soundness is now $\mathring{\alpha}^i_{\mathbb{F}}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}]\!]) \mathring{\sqsubseteq}^i \boldsymbol{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}]\!]$.
- However $\mathring{\sqsubseteq}^i$ in (32.26) is defined by concretization to $\wp(\mathbb{T}^{+\infty}_{\mathbb{V}})$.
- We look for a definition $\mathring{\sqsubseteq}^i$ in the abstract $\wp(\mathbb{T}^{+\infty}_{\mathbb{P}^i_{\mathbb{F}}})$ only, that provides a sufficient soundness condition $(\overline{\Pi} \mathring{\sqsubseteq}^i \overline{\Pi}') \Rightarrow (\overline{\Pi} \mathring{\sqsubseteq}^i \overline{\Pi}')$.

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).
- $\mathring{\sqsubseteq}^i$ is Hoare preorder [Winskel, 1983] on sets of traces.

$$\overline{\Pi} \mathrel{\mathring{\sqsubseteq}}^i \overline{\Pi}' \quad \triangleq \quad \forall \langle \overline{\pi}_0, \overline{\pi}_1 \rangle \in \overline{\Pi} \,.\, \exists \langle \overline{\pi}'_0, \overline{\pi}'_1 \rangle \in \overline{\Pi}' \,.\, \langle \overline{\pi}_0, \overline{\pi}_1 \rangle \mathrel{\ddot{\sqsubseteq}}^i \langle \overline{\pi}'_0, \overline{\pi}'_1 \rangle \tag{32.27}$$

where $\ddot{\sqsubseteq}^i$ is the pairwise extension of $\vec{\sqsubseteq}^i$

$$\langle \overline{\pi}_0, \overline{\pi}_1 \rangle \mathrel{\ddot{\sqsubseteq}}^i \langle \overline{\pi}'_0, \overline{\pi}'_1 \rangle \quad \triangleq \quad \overline{\pi}_0 \mathrel{\vec{\sqsubseteq}}^i \overline{\pi}'_0 \wedge \overline{\pi}_1 \mathrel{\vec{\sqsubseteq}}^i \overline{\pi}'_1$$

and $\vec{\sqsubseteq}^i$ is the tracewise extension of $\dot{\sqsubseteq}^i$, comparing traces of the same length, same control, but larger intervals.

$$\begin{aligned} \overline{\pi} \mathrel{\vec{\sqsubseteq}}^i \overline{\pi}' \quad \triangleq \quad & \text{let } \ell_1 \xrightarrow{\overline{\mathtt{a}}_1} \ell_2 \ldots \ell_n \xrightarrow{\overline{\mathtt{a}}_n} \ell_{n+1} \ldots = \overline{\pi} \\ & \text{and } \ell'_1 \xrightarrow{\overline{\mathtt{a}}'_1} \ell'_2 \ldots \ell'_n \xrightarrow{\overline{\mathtt{a}}'_n} \ell'_{n+1} \ldots = \overline{\pi}' \text{ in} \\ & \forall j \leqslant |\overline{\pi}| = |\overline{\pi}'| \,.\, \ell_j = \ell'_j \wedge \overline{\mathtt{a}}_j \mathrel{\dot{\sqsubseteq}}^i \overline{\mathtt{a}}'_j \end{aligned} \tag{32.28}$$

Sound over-approximation in the abstract(cont'd)

and the action intervals are larger

$$\begin{array}{rcl} (\mathsf{x} = \mathsf{A} = \overline{v}) \mathrel{\vec{\sqsubseteq}^i} (\mathsf{x} = \mathsf{A} = \overline{v}') & \triangleq & \overline{v} \sqsubseteq^i \overline{v}' \\ (\mathsf{B} = \overline{\rho}) \mathrel{\vec{\sqsubseteq}^i} (\mathsf{B} = \overline{\rho}') & \triangleq & \overline{\rho} \mathrel{\dot{\sqsubseteq}^i} \overline{\rho}' \\ (\neg(\mathsf{B}) = \overline{\rho}) \mathrel{\vec{\sqsubseteq}^i} (\neg(\mathsf{B}) = \overline{\rho}') & \triangleq & \overline{\rho} \mathrel{\dot{\sqsubseteq}^i} \overline{\rho}' \\ \mathsf{a} \mathrel{\vec{\sqsubseteq}^i} \mathsf{a} & & \text{for all other actions } \mathsf{a} \end{array} \tag{32.29}$$

- $\overline{\pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}'$ implies $\boldsymbol{\varrho}(\overline{\pi}) \mathrel{\dot{\sqsubseteq}^i} \boldsymbol{\varrho}(\overline{\pi}')$ (by (32.19) and (32.20)) and $\vec{\gamma}^i_{\mathbb{F}}(\overline{\pi}) \subseteq \vec{\gamma}^i_{\mathbb{F}}(\overline{\pi}')$ (32.30)
- $\mathrel{\mathring{\sqsubseteq}^i}$ allows for more abstract traces than $\mathrel{\vec{\sqsubseteq}^i}$:

  Lemma 3 $(\overline{\Pi} \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}') \Rightarrow (\overline{\Pi} \mathrel{\vec{\sqsubseteq}^i} \overline{\Pi}')$. □

Calculational design of the float interval trace semantics

- The float interval prefix trace semantics $\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ replaces concrete real or float traces (as defined by $\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]$) by interval traces.
- It is sound if and only if the concrete traces are included in the abstract traces that is $\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!] \dot{\subseteq} \mathring{\gamma}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!])$ or, equivalently, by (32.25), $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]) \dot{\subseteq} \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$.
- Although, the soundness condition $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]) \dot{\subseteq} \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ allows the abstract semantics $\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ to contain more traces, including with larger intervals, it requires the abstract traces in $\alpha^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!])$ (which are the best float interval abstractions of real computations) to all belong to the abstract semantics $\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$.
- We introduced $\mathring{\sqsubseteq}^i$ in (32.2) to relax this requirement about the presence of best interval trace abstractions of real computations in the abstract semantics.

Calculational design of the float interval trace semantics (cont'd)

- The weaker requirement $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\mathbb{E}}^i} \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ implies, by Lemma 3, that $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\sqsubseteq}^i} \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!])$ so that, by (32.26), $\mathring{\gamma}^i_{\mathbb{F}}(\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!])) \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!])$, which, together with $\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!] \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]))$ from the Galois connection (32.25) yields, by transitivity, that $\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!] \subseteq \mathring{\gamma}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!])$.
- This weaker soundness requirement $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]) \mathrel{\mathring{\mathbb{E}}^i} \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!])$ yields a calculational design method where $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!])$ is $\mathring{\mathbb{E}}^i$-over-approximated so as to eliminate any reference to the concrete semantics $\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}]\!]$.
- We proceed by structural induction on $\lhd$, assuming $\mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{s}']\!]) \mathrel{\mathring{\mathbb{E}}^i} \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}']\!]$ for all $\mathtt{s}' \lhd \mathtt{s}$.

Calculational design of the float interval trace semantics (cont'd)

- This is not a strong enough induction hypothesis to design $\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ such that $\mathring{\alpha}^i_{\mathbb{F}}(\boldsymbol{\mathcal{S}}_{\mathbb{R}}[\![\mathtt{s}]\!]) \mathbin{\mathring{\sqsubseteq}^i} \widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ by structural induction.
- In conjunction with $\mathring{\alpha}^i_{\mathbb{F}}(X) \mathbin{\mathring{\sqsubseteq}^i} \overline{X}$ stating that any concrete execution $\langle \pi, \pi' \rangle \in X$ has an abstraction $\langle \overline{\pi}, \overline{\pi}' \rangle$ in $\overline{X}$, we will need a stronger ind. hyp. stating that any sound abstraction $\overline{\pi}$ of a concrete prelude π (*i.e.* $\vec{\alpha}^i_{\mathbb{F}}(\pi) \mathbin{\vec{\sqsubseteq}^i} \overline{\pi}$) has an abstract continuation $\overline{\pi}'$ in $\overline{X}$ abstracting the concrete continuation π' (*i.e.* $\vec{\alpha}^i_{\mathbb{F}}(\pi') \mathbin{\vec{\sqsubseteq}^i} \overline{\pi}'$)
- Formally,

$$\forall \langle \pi, \pi' \rangle \in X \,.\, \forall \overline{\pi} \,.\, (\vec{\alpha}^i_{\mathbb{F}}(\pi) \mathbin{\vec{\sqsubseteq}^i} \overline{\pi}) \Rightarrow (\exists \overline{\pi}' \,.\, \langle \overline{\pi}, \overline{\pi}' \rangle \in \overline{X} \wedge \vec{\alpha}^i_{\mathbb{F}}(\pi') \mathbin{\vec{\sqsubseteq}^i} \overline{\pi}') \tag{32.32}$$

  which we will use for $X = \widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{V}}[\![\mathtt{s}]\!]$ and $\overline{X} = \widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]$ is well as for the concrete X and abstract $\overline{X}$ fixpoint iterates in (17.4) for iteration statements.

Interval trace semantics

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.

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\ell\ \mathtt{x = A\ ;}]\!] \quad \triangleq \quad \{\langle \overline{\pi}\ell,\ \ell\rangle\} \cup \{\langle \overline{\pi}\ell,\ \ell \xrightarrow{\mathtt{x = A} = \overline{\nu}} \mathrm{after}[\![\mathtt{S}]\!]\rangle \mid \overline{\nu} = \mathcal{A}^{i}_{\mathbb{F}}[\![\mathtt{A}]\!]\varrho(\overline{\pi}\ell)\}$$

Interval trace semantics of a break statement

For a break statement $\mathtt{S} = \ell\ \mathtt{break}\ \mathtt{;}$, we discover, by calculational design, that

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\mathtt{S}]\!] \quad \triangleq \quad \{\langle \overline{\pi}^{\ell},\ \ell \rangle\} \cup \{\langle \overline{\pi}^{\ell},\ \ell \xrightarrow{\mathtt{break}} \text{break-to}[\![\mathtt{S}]\!] \rangle\}$$

Interval trace semantics of the statement list

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{sl}]\!] \triangleq \{\langle \overline{\pi} \mathrm{at}[\![\mathtt{sl}]\!], \mathrm{at}[\![\mathtt{sl}]\!]\rangle \mid \overline{\pi}\mathrm{at}[\![\mathtt{sl}]\!] \in \mathbb{T}^{+}_{\mathbb{P}^i_{\mathbb{F}}}\} \qquad \mathtt{sl} ::= \epsilon$$

$$\triangleq \widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{sl}']\!] \cup \{\langle \overline{\pi}_1, \overline{\pi}_2 \frown \overline{\pi}_3\rangle \mid \langle \overline{\pi}_1, \overline{\pi}_2\rangle \in \widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{sl}']\!]) \wedge \langle \overline{\pi}_1 \frown \overline{\pi}_2, \overline{\pi}_3\rangle \in \widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{s}]\!]\} \qquad \mathtt{sl} ::= \mathtt{sl}'\ \mathtt{s}$$

Interval trace semantics of a conditional statement

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{if}^{\ell}\ \texttt{(B)}\ \mathtt{S}_t]\!] \triangleq \{\langle\overline{\pi}\ell,\ \ell\rangle \mid \overline{\pi}\ell \in \mathbb{T}^{+}_{\mathbb{P}^i_{\mathbb{R}}}\} \cup \tag{32.33}$$

$$\{\langle\overline{\pi}\ell,\ \ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \mathsf{after}[\![\mathtt{S}]\!]\rangle \mid \exists\overline{\rho}_{\mathtt{tt}}\ .\ \mathscr{B}^{i}_{\mathbb{F}}[\![\mathtt{B}]\!]\varrho(\overline{\pi}\ell) = \langle\overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\}^{1} \cup$$

$$\{\langle\overline{\pi}\ell,\ \ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathtt{S}_t]\!] \frown \overline{\pi}'\rangle \mid \exists\overline{\rho}_{\mathtt{ff}}\ .\ \mathscr{B}^{i}_{\mathbb{F}}[\![\mathtt{B}]\!]\varrho(\overline{\pi}\ell) = \langle\overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge$$

$$\langle\overline{\pi}\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathtt{S}_t]\!],\ \overline{\pi}'\rangle \in \widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_t]\!]\}^{2}$$

(and similarly for $\texttt{if}^{\ell}\ \texttt{(B)}\ \mathtt{S}_t\ \texttt{else}\ \mathtt{S}_f$)

[1] If $\dot{\gamma}^{i}_{\mathbb{F}}(\dot{\varnothing}) = \varnothing$ then this case is $\varnothing$ when $\overline{\rho}_{\mathtt{ff}} = \dot{\varnothing}$.

[2] If $\dot{\gamma}^{i}_{\mathbb{F}}(\dot{\varnothing}) = \varnothing$ then this case is $\varnothing$ when $\overline{\rho}_{\mathtt{tt}} = \dot{\varnothing}$.

Interval trace semantics of the iteration statement

$$\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\ell}\ (\texttt{B})\ \texttt{S}_b]\!] \;=\; \mathrm{lfp}^{\dot{\subseteq}}\, \mathscr{F}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\ell}\ (\texttt{B})\ \texttt{S}_b]\!]$$

$$\mathscr{F}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\ell}\ (\texttt{B})\ \texttt{S}_b]\!]\, X \;\triangleq\; \{\langle \overline{\pi}^{\ell},\ \ell\rangle \mid \overline{\pi}^{\ell} \in \mathbb{T}^+_{\mathbb{P}^i_{\mathbb{R}}}\} \qquad (32.34)$$

$$\cup\, \{\langle \overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell} \xrightarrow{\neg(\texttt{B}) = \overline{\rho}_{\texttt{ff}}} \mathrm{after}[\![\texttt{S}]\!]\rangle \mid \langle \overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell}\rangle \in X \wedge \exists \overline{\rho}_{\texttt{tt}}\ .$$
$$\mathscr{B}^i_{\mathbb{F}}[\![\texttt{B}]\!]\boldsymbol{\varrho}(\overline{\pi}_1{}^{\ell}\overline{\pi}_2{}^{\ell}) = \langle \overline{\rho}_{\texttt{tt}},\ \overline{\rho}_{\texttt{ff}}\rangle\}$$[3]

$$\cup\, \{\langle \overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell} \xrightarrow{\texttt{B} = \overline{\rho}_{\texttt{tt}}} \mathrm{at}[\![\texttt{S}_b]\!] \frown \overline{\pi}_3\rangle \mid \langle \overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell}\rangle \in X \wedge \exists \overline{\rho}_{\texttt{ff}}\ .$$
$$\mathscr{B}^i_{\mathbb{F}}[\![\texttt{B}]\!]\boldsymbol{\varrho}(\overline{\pi}_1{}^{\ell}\overline{\pi}_2{}^{\ell}) = \langle \overline{\rho}_{\texttt{tt}},\ \overline{\rho}_{\texttt{ff}}\rangle \wedge \langle \overline{\pi}_1{}^{\ell}\overline{\pi}_2{}^{\ell} \xrightarrow{\texttt{B} = \rho_{\texttt{tt}}} \mathrm{at}[\![\texttt{S}_b]\!],\ \overline{\pi}_3\rangle \in \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{S}_b]\!]\}$$[4]

[3] If $\dot{\gamma}^i_{\mathbb{F}}(\dot{\varnothing}) = \varnothing$ then this case is $\varnothing$ when $\overline{\rho}_{\texttt{ff}} = \dot{\varnothing}$.

[4] If $\dot{\gamma}^i_{\mathbb{F}}(\dot{\varnothing}) = \varnothing$ then this case is $\varnothing$ when $\overline{\rho}_{\texttt{tt}} = \dot{\varnothing}$.

Comparison of the float and interval semantics

- In conclusion of this section, $\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}$ is similar to $\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{V}}$ in (6.11)—(6.30), except for statements involving tests for which we have (32.33) for the conditional and (32.34) for the iteration statement.

Conclusion

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 [Damouche, Martel, and Chapoutot, 2018; Delmas, Goubault, Putot, Souyris, Tekkal, and Védrine, 2009; Ghorbal, Goubault, and Putot, 2009; Goubault and Putot, 2006, 2015, 2019; Goubault, Putot, Baufreton, and Gassino, 2007; Goubault, Putot, and Sahlmann, 2018; Goubault, Putot, and Védrine, 2012; Martel, 2011].
- Fluctuat can be used to compare a program run with reals and floats

en.wikipedia.org/wiki/Fluctuat

On floating point computations (cont'd)

- 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.* [Isaacson and Keller, 1994, pp. 91–94]).

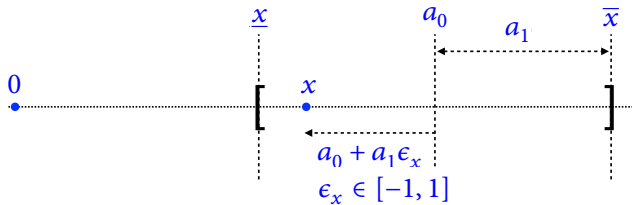
Affine arithmetic

- Interval arithmetic is imprecise.
- For example, if $x \in [1, 4]$ then $x - x \in [1 - 4, 4 - 1] = [-3, 3]$ instead of $[0, 0]$.
- The problem as that the arguments of functions cannot be correlated by a cartesian abstraction.
- So we have to independently take into consideration all possible values of variables within their interval of variation.
- And the problem cumulates over time along traces.
- Several solutions have been proposed to solves this imprecision problem [Nedialkov, Kreinovich, and Starks, 2004].

Affine arithmetic (cont'd)

- One of them, *affine arithmetics* [Comba and Stolfi, 1993; Stolfi and Figueiredo, 2003], represents an interval $x \in [\underline{x}, \overline{x}]$ by

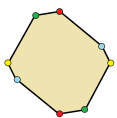
  $x = a_0 + a_1\epsilon_x$ where $a_0 = \frac{\overline{x}+\underline{x}}{2}$, $a_1 = \frac{\overline{x}-\underline{x}}{2}$, and $\epsilon_x \in [-1, 1]$ is a fresh auxiliary variable.



- Then $x - x = (a_0 + a_1\epsilon_x) - (a_0 + a_1\epsilon_x) = 0 + 0\epsilon_x$, as required.

Affine arithmetic (cont'd)

- In general a program involves several variables so we have an affine form $x = a_0 + a_1\epsilon_1 + a_2\epsilon_2 + \cdots + a_n\epsilon_n$.
- This implies $x \in [a_0 - d, a_0 + d]$ where $d = \sum_{i=1}^{n} |a_i|$ is the total deviation of x.
- This is, by interval arithmetic, the smallest interval that contains all possible values of x, assuming that each ϵ_i ranges independently over the interval $[-1, +1]$.
- For m variables, the affine constraints determine a *zonotope* [McMullen, 1971], a center-symmetric convex polytope in $\mathbb{R}^m$, whose faces are themselves center-symmetric [Beck and Robins, 2015, Ch. 9].



Example of zonotope: octagonal zonogon

- As was the case for interval arithmetic, zonotope arithmetic is an abstract interpretation of the real/float semantics (used in Fluctuat).

en.wikipedia.org/wiki/Zonohedron#Zonotopes

Conclusion

- Interval arithmetic in scientific computing put bounds on rounding errors in floating point arithmetic [Moore, 1966].
- Interval arithmetic in scientific computing is an abstract interpretation of the trace semantics of Chapters **6** and **7** so can be computed at runtime for one trace at a time (*i.e.* during one program execution).
- Tests may have to consider many executions, which can be quite inefficient (and often considered an error in practice).
- We study static interval analysis in next Chapter **33**. This is a cartesian abstraction of Chapter **32** that is an abstraction of the reachability semantics of Chapter **19** (itself an abstraction of the trace semantics of Chapters **6** and **7**).
- Static interval analysis cannot be performed at runtime since it must deal with all possible program computation traces in finite time.

Bibliography I

Beck, Matthias and Sinai Robins (2015). *Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra*. 2nd ed. Undergraduate Texts in Mathematics. Springer.

Comba, João Luiz Dihl and Jorge Stolfi (1993). "Affine arithmetic and its applications to computer graphics". *SIBGRAPI*, pp. 9–18.

Damouche, Nasrine, Matthieu Martel, and Alexandre Chapoutot (2018). "Numerical program optimisation by automatic improvement of the accuracy of computations". *IJIEI* 6.1/2, pp. 115–145.

Darulova, Eva and Viktor Kuncak (2017). "Towards a Compiler for Reals". *ACM Trans. Program. Lang. Syst.* 39.2, 8:1–8:28.

de Figueiredo, Luiz Henrique and Jorge Stolfi (2004). "Affine Arithmetic: Concepts and Applications". *Numerical Algorithms* 37.1-4, pp. 147–158.

Bibliography II

Delmas, David, Éric Goubault, Sylvie Putot, Jean Souyris, Karim Tekkal, and Franck Védrine (2009). "Towards an Industrial Use of FLUCTUAT on Safety-Critical Avionics Software". In: *FMICS*. Vol. 5825. Lecture Notes in Computer Science. Springer, pp. 53–69.

Gange, Graeme, Jorge A. Navas, Peter Schachte, Harald Søndergaard, and Peter J. Stuckey (2014). "Interval Analysis and Machine Arithmetic: Why Signedness Ignorance Is Bliss". *ACM Trans. Program. Lang. Syst.* 37.1, 1:1–1:35.

Ghorbal, Khalil, Éric Goubault, and Sylvie Putot (2009). "The Zonotope Abstract Domain Taylor1+". In: *CAV*. Vol. 5643. Lecture Notes in Computer Science. Springer, pp. 627–633.

Goldberg, David (1991). "What Every Computer Scientist Should Know About Floating-Point Arithmetic". *ACM Comput. Surv.* 23.1, pp. 5–48.

Bibliography III

Goubault, Éric and Sylvie Putot (2006). "Static Analysis of Numerical Algorithms". In: *SAS*. Vol. 4134. Lecture Notes in Computer Science. Springer, pp. 18–34.

— (2015). "A zonotopic framework for functional abstractions". *Formal Methods in System Design* 47.3, pp. 302–360.

— (2019). "Inner and outer reachability for the verification of control systems". In: *HSCC*. ACM, pp. 11–22.

Goubault, Éric, Sylvie Putot, Philippe Baufreton, and Jean Gassino (2007). "Static Analysis of the Accuracy in Control Systems: Principles and Experiments". In: *FMICS*. Vol. 4916. Lecture Notes in Computer Science. Springer, pp. 3–20.

Goubault, Éric, Sylvie Putot, and Lorenz Sahlmann (2018). "Inner and Outer Approximating Flowpipes for Delay Differential Equations". In: *CAV (2)*. Vol. 10982. Lecture Notes in Computer Science. Springer, pp. 523–541.

Bibliography IV

Goubault, Éric, Sylvie Putot, and Franck Védrine (2012). "Modular Static Analysis with Zonotopes". In: *SAS*. Vol. 7460. Lecture Notes in Computer Science. Springer, pp. 24–40.

Hickey, Timothy J., Qun Ju, and Maarten H. van Emden (2001). "Interval arithmetic: From principles to implementation". *J. ACM* 48.5, pp. 1038–1068.

IEEE (1985). *IEEE Standard for Binary Floating-Point Arithmetic*. American National Standards Institute, Institute of Electrical, and Electronic Engineers, ANSI/IEEE Standard 754-1985.

Isaacson, Eugene and Herbert Bishop Keller (1994). *Analysis of Numerical Methods*. Dover Books on Mathematics.

Martel, Matthieu (2011). "RangeLab: A Static-Analyzer to Bound the Accuracy of Finite-Precision Computations". In: *SYNASC*. IEEE Computer Society, pp. 118–122.

McMullen, Peter (1971). "On zonotopes". *Trans. Amer. Math. Soc.* 159, pp. 91–110.

Bibliography V

Monniaux, David (2008). "The pitfalls of verifying floating-point computations". *ACM Trans. Program. Lang. Syst.* 30.3, 12:1–12:41.

Moore, Ramon E. (1966). *Interval analysis*. Prentice Hall.

Moore, Ramon E., R. Baker Kearfott, and Michael J. Cloud (Mar. 2009). *Introduction to Interval Analysis*. Society for Industrial and Applied Mathematics.

Müller-Olm, Markus and Helmut Seidl (2005). "Analysis of Modular Arithmetic". In: *ESOP*. Vol. 3444. Lecture Notes in Computer Science. Springer, pp. 46–60.

Nedialkov, Nedialko S., Vladik Kreinovich, and Scott A. Starks (2004). "Interval Arithmetic, Affine Arithmetic, Taylor Series Methods: Why, What Next?" *Numerical Algorithms* 37.1-4, pp. 325–336.

Simon, Axel and Andy King (2007). "Taming the Wrapping of Integer Arithmetic". In: *SAS*. Vol. 4634. Lecture Notes in Computer Science. Springer, pp. 121–136.

Bibliography VI

Stolfi, Jorge and Luiz Henrique de Figueiredo (2003). "An Introduction to Affine Arithmetic". *TEMA Tend. Mat. Apl. Comput.* 4.3, pp. 297–312.

Winskel, Glynn (1983). "A Note on Powerdomains and Modalitiy". In: *FCT*. Vol. 158. Lecture Notes in Computer Science. Springer, pp. 505–514.

Soundness of the interval trace semantics

Interval trace semantics of an assignment statement $\mathtt{S} = \ell\ \mathtt{x = A\ ;}$

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

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\ell\ \mathtt{x = A\ ;}]\!] \quad \triangleq \quad \{\langle \overline{\pi}\ell,\ \ell\rangle\} \cup \{\langle \overline{\pi}\ell,\ \ell \xrightarrow{\mathtt{x = A} = \overline{\nu}} \mathrm{after}[\![\mathtt{S}]\!]\rangle \mid \overline{\nu} = \mathcal{A}^{i}_{\mathbb{F}}[\![\mathtt{A}]\!]\varrho(\overline{\pi}\ell)\}$$

Proof I

$$
\begin{aligned}
& \mathring{\alpha}^i_{\mathbb{F}}(\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\ell\ \texttt{x = A ;}]\!]) \\
= \ & \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi,\ \pi' \rangle) \mid \langle \pi,\ \pi' \rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\ell\ \texttt{x = A ;}]\!]\} && \text{⟅set of traces abstraction (32.24)⟆} \\
= \ & \{\langle \vec{\alpha}^i_{\mathbb{F}}(\pi),\ \vec{\alpha}^i_{\mathbb{F}}(\pi') \rangle \mid \langle \pi,\ \pi' \rangle \in \{\langle \pi\ell,\ \ell \rangle\} \cup \{\langle \pi\ell,\ \ell \xrightarrow{\texttt{x = A} = \nu} \text{after}[\![\texttt{S}]\!] \rangle \mid \nu = \mathcal{A}[\![\texttt{A}]\!]\rho(\pi\ell)\}\} \\
& && \text{⟅def. (32.23) of } \ddot{\vec{\alpha}}^i_{\mathbb{F}} \text{ and def. } \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\ell\ \texttt{x = A ;}]\!] \text{ in (17.2)⟆} \\
= \ & \{\langle \vec{\alpha}^i_{\mathbb{F}}(\pi\ell),\ \ell \rangle\} \cup \{\langle \vec{\alpha}^i_{\mathbb{F}}(\pi\ell),\ \ell \xrightarrow{\texttt{x = A} = \overline{\nu}} \text{after}[\![\texttt{S}]\!] \rangle \mid \overline{\nu} = \alpha^i_{\mathbb{F}}(\mathcal{A}[\![\texttt{A}]\!]\rho(\pi\ell))\} \\
& && \text{⟅def. } \in \text{ and def. (32.20) and (32.21) of trace abstraction⟆} \\
\mathring{\mathbb{E}}^i \ & \{\langle \vec{\alpha}^i_{\mathbb{F}}(\pi\ell),\ \ell \rangle\} \cup \{\langle \vec{\alpha}^i_{\mathbb{F}}(\pi\ell),\ \ell \xrightarrow{\texttt{x = A} = \overline{\nu}} \text{after}[\![\texttt{S}]\!] \rangle \mid \overline{\nu} = \mathcal{A}^i_{\mathbb{F}}[\![\texttt{A}]\!](\dot{\alpha}^i_{\mathbb{F}}(\rho(\pi\ell)))\} \\
& && \text{⟅(32.16) and def. (32.27) of } \mathring{\mathbb{E}}^i \text{⟆} \\
\mathring{\mathbb{E}}^i \ & \{\langle \overline{\pi}\ell,\ \ell \rangle\} \cup \{\langle \overline{\pi}\ell,\ \ell \xrightarrow{\texttt{x = A} = \overline{\nu}} \text{after}[\![\texttt{S}]\!] \rangle \mid \overline{\nu} = \mathcal{A}^i_{\mathbb{F}}[\![\texttt{A}]\!]\rho(\overline{\pi}\ell)\} \\
& && \text{⟅letting } \overline{\pi}\ell = \vec{\alpha}^i_{\mathbb{F}}(\pi\ell) \text{ so } \dot{\alpha}^i_{\mathbb{F}}(\rho(\pi\ell)) = \rho(\overline{\pi}\ell) \text{ and def. (32.27) of } \mathring{\mathbb{E}}^i \text{⟆} \\
\triangleq \ & \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\ell\ \texttt{x = A ;}]\!] && \text{⟅by defining } \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\ell\ \texttt{x = A ;}]\!] \text{ as in (17.2) for } \mathbb{V} = \mathbb{P}^i_{\mathbb{F}}\text{⟆}
\end{aligned}
$$

Proof II

- Assume that $\langle \pi, \pi' \rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\ell \ \mathtt{x = A\ ;}]\!]$ and $\vec{\alpha}^i_{\mathbb{F}}(\pi) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}$
- By def. $\widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\ell \ \mathtt{x = A\ ;}]\!]$ in (17.2), it follows that the trace π ends at ℓ and either $\pi' = \ell$ (which is a trivial case) or else $\pi' = \ell \xrightarrow{\mathtt{x = A} = \mathcal{A}[\![\mathtt{A}]\!]\varrho(\pi)} \mathrm{after}[\![\mathtt{S}]\!]$
- Since the trace π ends at ℓ, the hypothesis $\vec{\alpha}^i_{\mathbb{F}}(\pi) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}$ implies that $\overline{\pi}$ ends at ℓ, and so there exists $\overline{\pi}'$ *s.t.* $\langle \overline{\pi}, \overline{\pi}' \rangle \in \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\ell \ \mathtt{x = A\ ;}]\!]$ with $\overline{\pi}' = \ell \xrightarrow{\mathtt{x = A} = \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\varrho(\overline{\pi})} \mathrm{after}[\![\mathtt{S}]\!]$. Now

$$
\begin{array}{ll}
& \bar{\alpha}^i_{\mathbb{F}}(\mathtt{x = A} = \mathcal{A}[\![\mathtt{A}]\!]\varrho(\pi)) \\
= & \mathtt{x = A} = \alpha^i_{\mathbb{F}}(\mathcal{A}[\![\mathtt{A}]\!]\varrho(\pi)) \qquad \wr \text{def. (32.20) of } \bar{\alpha}^i_{\mathbb{F}} \wr \\
\mathrel{\dot{\sqsubseteq}^i} & \mathtt{x = A} = \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\dot{\alpha}^i_{\mathbb{F}}(\varrho(\pi)) \qquad \wr \alpha^i_{\mathbb{F}}(\mathcal{A}_{\mathbb{V}}[\![\mathtt{A}]\!]\rho) \sqsubseteq^i \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\dot{\alpha}^i_{\mathbb{F}}(\rho) \text{ by (32.16) and def. } \dot{\sqsubseteq}^i \wr \\
\mathrel{\dot{\sqsubseteq}^i} & \mathtt{x = A} = \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\varrho(\vec{\alpha}^i_{\mathbb{F}}(\pi)) \qquad \wr \dot{\alpha}^i_{\mathbb{F}}(\varrho(\pi)) \mathrel{\dot{\sqsubseteq}^i} \varrho(\vec{\alpha}^i_{\mathbb{F}}(\pi)) \text{ by (32.22) and } \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!] \text{ increasing} \wr \\
\mathrel{\dot{\sqsubseteq}^i} & \mathtt{x = A} = \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\varrho(\overline{\pi}) \quad \wr \vec{\alpha}^i_{\mathbb{F}}(\pi) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi} \text{ so } \varrho(\vec{\alpha}^i_{\mathbb{F}}(\pi)) \sqsubseteq^i \varrho(\overline{\pi}) \text{ by (32.30) and } \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!] \text{ increasing} \wr
\end{array}
$$

- By def. (32.28) of $\vec{\sqsubseteq}^i$, it follows that $\vec{\alpha}^i_{\mathbb{F}}(\pi') = \ell \xrightarrow{\bar{\alpha}^i_{\mathbb{F}}(\mathtt{x = A} = \mathcal{A}[\![\mathtt{A}]\!]\varrho(\pi))} \mathrm{after}[\![\mathtt{S}]\!] \mathrel{\vec{\sqsubseteq}^i} \ell \xrightarrow{\mathtt{x = A} = \mathcal{A}^i_{\mathbb{F}}[\![\mathtt{A}]\!]\varrho(\overline{\pi})} \mathrm{after}[\![\mathtt{S}]\!] = \overline{\pi}'$, proving (32.32). □

Interval trace semantics of a conditional statement

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{if}^{\ell}\ \texttt{(B)}\ \mathtt{S}_t]\!] \triangleq \{\langle \overline{\pi}\ell,\ \ell\rangle \mid \overline{\pi}\ell \in \mathbb{T}^{+}_{\mathbb{P}^i_{\mathbb{R}}}\} \cup \tag{32.33}$$

$$\{\langle \overline{\pi}\ell,\ \ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \mathrm{after}[\![\mathtt{S}]\!]\rangle \mid \exists \overline{\rho}_{\mathtt{tt}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\varrho(\overline{\pi}\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\} \cup$$

$$\{\langle \overline{\pi}\ell,\ \ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!] \frown \overline{\pi}'\rangle \mid \exists \overline{\rho}_{\mathtt{ff}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\varrho(\overline{\pi}\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge$$

$$\langle \overline{\pi}\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!],\ \overline{\pi}'\rangle \in \widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_t]\!]\}$$

(and similarly for $\texttt{if}^{\ell}\ \texttt{(B)}\ \mathtt{S}_t\ \texttt{else}\ \mathtt{S}_f$)

Proof I

We can now abstract the semantics of real tests using float intervals.

$$\mathring{\alpha}^i_{\mathbb{F}}(\overline{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{if } \ell \texttt{ (B) } \mathsf{S}_t]\!])$$

$$\triangleq \mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi^\ell, \ell\rangle \mid \pi^\ell \in \mathbb{T}^+_{\mathbb{R}}\} \cup \{\langle \pi^\ell, \ell \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathrm{ff}\} \cup \{\langle \pi^\ell, \ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathrm{tt} \wedge \langle \pi^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathsf{S}_t]\!], \pi'\rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}_t]\!]\})$$

〈(6.11), (6.18), (6.19), Section **16.3.1**, and Section **32.5.5**〉

$$= \mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi^\ell, \ell\rangle \mid \pi^\ell \in \mathbb{T}^+_{\mathbb{R}}\}) \cup \mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi^\ell, \ell \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathrm{ff}\}) \cup \mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi^\ell, \ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathrm{tt} \wedge \langle \pi^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathsf{S}_t]\!], \pi'\rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}_t]\!]\})$$

〈join preservation in (32.25)〉

$$= \{\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi^\ell, \ell\rangle) \mid \pi^\ell \in \mathbb{T}^+_{\mathbb{R}}\} \cup \{\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi^\ell, \ell \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{after}[\![\mathsf{S}]\!]\rangle) \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathrm{ff}\} \cup \{\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi^\ell, \ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle) \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathrm{tt} \wedge \langle \pi^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathsf{S}_t]\!], \pi'\rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}_t]\!]\}$$

〈def. (32.24) of $\mathring{\alpha}^i_{\mathbb{F}}$〉

Proof II

$$\{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell\rangle) \mid \pi^\ell \in \mathbb{T}^+_{\mathbb{R}}\} \cup \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{after}[\![\mathsf{S}]\!]\rangle) \mid \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathtt{ff}\} \cup \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,$$
$$\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle) \mid \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathtt{tt} \wedge \langle \pi^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{at}[\![\mathsf{S}_t]\!],\ \pi'\rangle \in \widehat{\mathscr{S}}^*_{\mathbb{V}}[\![\mathsf{S}_t]\!]\}$$

$$\mathring{\ddot{\mathbb{E}}}^i\ \{\langle \overline{\pi}^\ell,\ \ell\rangle \mid \overline{\pi}^\ell \in \mathbb{T}^+_{\mathbb{P}^i_{\mathbb{R}}}\} \cup \{\langle \overline{\pi}^\ell,\ \ell \xrightarrow{\neg(\mathsf{B}) = \overline{\rho}_{\mathtt{ff}}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \exists \overline{\rho}_{\mathtt{tt}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\} \cup \{\langle \overline{\pi}^\ell,$$
$$\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \overline{\pi}'\rangle \mid \exists \overline{\rho}_{\mathtt{ff}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge \langle \overline{\pi}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathsf{S}_t]\!],\ \overline{\pi}'\rangle \in \widehat{\mathscr{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathsf{S}_t]\!]\}$$

⟅— For the first term, by def. (32.27) of $\mathring{\ddot{\mathbb{E}}}^i$, we must prove that $\forall \ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell\rangle)\ .\ \exists \langle \overline{\pi}^\ell,\ \ell\rangle\ .\ \ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell\rangle)\ \ddot{\vec{\mathbb{E}}}^i\ \langle \overline{\pi}^\ell,\ \ell\rangle$. We can simply choose $\overline{\pi}^\ell = \vec{\alpha}^i_{\mathbb{F}}(\pi^\ell)$.

Proof III

$$\{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell\rangle) \mid \pi^\ell \in \mathbb{T}^+_{\mathbb{R}}\} \cup \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell \xrightarrow{\neg(\mathtt{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{after}[\![\mathtt{S}]\!]\rangle) \mid \mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathtt{ff}\} \cup \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,$$
$$\ell \xrightarrow{\mathtt{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathtt{S}_t]\!] \frown \pi'\rangle) \mid \mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathtt{tt} \wedge \langle \pi^\ell \xrightarrow{\mathtt{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathtt{S}_t]\!],\ \pi'\rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}_t]\!]\}$$

$$\mathring{\mathbb{E}}^i\ \{\langle \overline{\pi}^\ell,\ \ell\rangle \mid \overline{\pi}^\ell \in \mathbb{T}^+_{\mathbb{P}^i_{\mathbb{R}}}\} \cup \{\langle \overline{\pi}^\ell,\ \ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \mathrm{after}[\![\mathtt{S}]\!]\rangle \mid \exists \overline{\rho}_{\mathtt{tt}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\} \cup \{\langle \overline{\pi}^\ell,$$
$$\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!] \frown \overline{\pi}'\rangle \mid \exists \overline{\rho}_{\mathtt{ff}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge \langle \overline{\pi}^\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!],\ \overline{\pi}'\rangle \in \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_t]\!]\}$$

— For the second term, by def. (32.27) of $\mathring{\mathbb{E}}^i$, we must prove that $\forall \ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,$
$\ell \xrightarrow{\neg(\mathtt{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{after}[\![\mathtt{S}]\!]\rangle) = \langle \vec{\alpha}^i_{\mathbb{F}}(\pi^\ell),\ \ell \xrightarrow{\neg(\mathtt{B}) = \dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi^\ell))} \mathrm{after}[\![\mathtt{S}]\!]\rangle\ .\ \exists \langle \overline{\pi}^\ell,$
$\ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \mathrm{after}[\![\mathtt{S}]\!]\rangle\ .\ \langle \dot{\alpha}^i_{\mathbb{F}}(\pi^\ell),\ \ell \xrightarrow{\neg(\mathtt{B}) = \dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi^\ell))} \mathrm{after}[\![\mathtt{S}]\!]\rangle \ddot{\mathbb{E}}^i \langle \overline{\pi}^\ell,\ \ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}}$
$\mathrm{after}[\![\mathtt{S}]\!]\rangle$.

The control abstraction is the same.

We can choose $\overline{\pi}^\ell = \vec{\alpha}^i_{\mathbb{F}}(\pi^\ell)$ so that $\mathscr{B}_{\mathbb{V}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathtt{ff}$, (32.18), and $\mathscr{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}}\rangle$ imply that $\dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi^\ell)) \sqsubseteq^i \overline{\rho}_{\mathtt{ff}}$.

Proof IV

$$\{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell\rangle) \mid \pi^\ell \in \mathbb{T}^+_{\mathbb{R}}\} \cup \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{after}[\![\mathsf{S}]\!]\rangle) \mid \boldsymbol{\mathscr{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathit{ff}\} \cup \{\ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle) \mid \boldsymbol{\mathscr{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathit{tt} \wedge \langle \pi^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{at}[\![\mathsf{S}_t]\!],\ \pi'\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{V}}[\![\mathsf{S}_t]\!]\}$$

$$\mathring{\mathbb{E}}^i\ \{\langle \overline{\pi}^\ell,\ \ell\rangle \mid \overline{\pi}^\ell \in \mathbb{T}^+_{\mathbb{P}^i_{\mathbb{R}}}\} \cup \{\langle \overline{\pi}^\ell,\ \ell \xrightarrow{\neg(\mathsf{B}) = \overline{\rho}_{\mathit{ff}}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \exists \overline{\rho}_{\mathit{tt}}\ .\ \boldsymbol{\mathscr{B}}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathit{tt}},\ \overline{\rho}_{\mathit{ff}}\rangle\} \cup \{\langle \overline{\pi}^\ell,\ \ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathit{tt}}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \overline{\pi}'\rangle \mid \exists \overline{\rho}_{\mathit{ff}}\ .\ \boldsymbol{\mathscr{B}}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathit{tt}},\ \overline{\rho}_{\mathit{ff}}\rangle \wedge \langle \overline{\pi}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathit{tt}}} \mathsf{at}[\![\mathsf{S}_t]\!],\ \overline{\pi}'\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathsf{S}_t]\!]\}$$

— For the third term, by def. (32.27) of $\mathring{\mathbb{E}}^i$, we must prove that $\forall \ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle) = \langle \vec{\alpha}^i_{\mathbb{F}}(\pi^\ell),\ \ell \xrightarrow{\mathsf{B} = \dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi^\ell))} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \vec{\alpha}^i_{\mathbb{F}}(\pi')\rangle\ .\ \exists \langle \overline{\pi}^\ell,\ \ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathit{tt}}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \overline{\pi}'\rangle\ .\ \ddot{\vec{\alpha}}^i_{\mathbb{F}}(\langle \pi^\ell,\ \ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \pi'\rangle) \ddot{\mathbb{E}}^i \langle \overline{\pi}^\ell,\ \ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathit{tt}}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \overline{\pi}'\rangle$.

The control abstraction is the same.

We can choose $\overline{\pi}^\ell = \vec{\alpha}^i_{\mathbb{F}}(\pi^\ell)$ so that $\boldsymbol{\mathscr{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi^\ell) = \mathit{tt}$, (32.18), and $\boldsymbol{\mathscr{B}}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^\ell) = \langle \overline{\rho}_{\mathit{tt}},\ \overline{\rho}_{\mathit{ff}}\rangle$ imply that $\dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi^\ell)) \dot{\mathbb{E}}^i \overline{\rho}_{\mathit{tt}}$.

Proof V

It remains to find $\overline{\pi}'$ such that $\vec{\alpha}^i_{\mathbb{F}}(\pi') \vec{\sqsubseteq}^i \overline{\pi}'$ and $\langle \overline{\pi}^\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!], \overline{\pi}' \rangle \in \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_t]\!]$.

It is given by the induction hypothesis (32.32) where $\langle \pi^\ell \xrightarrow{\mathtt{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathtt{S}_t]\!], \pi' \rangle \in \widehat{\mathcal{S}}^*_{\mathbb{V}}[\![\mathtt{S}_t]\!]$ and $\vec{\alpha}^i_{\mathbb{F}}(\pi^\ell \xrightarrow{\mathtt{B} = \boldsymbol{\varrho}(\pi^\ell)} \mathrm{at}[\![\mathtt{S}_t]\!]) \vec{\sqsubseteq}^i \overline{\pi}^\ell \xrightarrow{\mathtt{B} = \boldsymbol{\varrho}(\overline{\pi}^\ell)_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!]$ imply that $\exists \overline{\pi}' \,.\, \langle \overline{\pi}^\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_t]\!], \overline{\pi}' \rangle \in \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_t]\!] \wedge \vec{\alpha}^i_{\mathbb{F}}(\pi') \vec{\sqsubseteq}^i \overline{\pi}' \,.\, \wr$

$\triangleq \widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{if}^{\,\ell}\ \mathtt{(B)}\ \mathtt{S}_t]\!]$

$\wr$since the above term involves only computations in $\mathbb{S}_{\mathbb{P}^i}$ and none in $\mathbb{S}_{\mathbb{V}}\wr$

It remains to show that $\widehat{\mathcal{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{if}^{\,\ell}\ \mathtt{(B)}\ \mathtt{S}_t]\!]$ satisfies (32.32), which is trivial for the first two terms. For the third term, this follows from the induction hypothesis. □

Interval trace semantics of the iteration statement

$$\widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\ell}\ (\mathtt{B})\ \mathtt{S}_b]\!] \quad = \quad \mathrm{lfp}^{\dot{\subseteq}}\, \mathcal{F}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\ell}\ (\mathtt{B})\ \mathtt{S}_b]\!]$$

$$\mathcal{F}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\ell}\ (\mathtt{B})\ \mathtt{S}_b]\!]\, X \quad \triangleq \quad \{\langle \overline{\pi}\ell,\ \ell\rangle \mid \overline{\pi}\ell \in \mathbb{T}^{+}_{\mathbb{P}^i_{\mathbb{R}}}\} \tag{32.34}$$

$$\cup \{\langle \overline{\pi}_1\ell,\ \ell\overline{\pi}_2\ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \mathrm{after}[\![\mathtt{S}]\!]\rangle \mid \langle \overline{\pi}_1\ell,\ \ell\overline{\pi}_2\ell\rangle \in X \wedge \exists \overline{\rho}_{\mathtt{tt}}\ .$$

$$\mathcal{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\varrho(\overline{\pi}_1\ell\overline{\pi}_2\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\}$$[5]

$$\cup \{\langle \overline{\pi}_1\ell,\ \ell\overline{\pi}_2\ell \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_b]\!] \frown \overline{\pi}_3\rangle \mid \langle \overline{\pi}_1\ell,\ \ell\overline{\pi}_2\ell\rangle \in X \wedge \exists \overline{\rho}_{\mathtt{ff}}\ .$$

$$\mathcal{B}^i_{\mathbb{F}}[\![\mathtt{B}]\!]\varrho(\overline{\pi}_1\ell\overline{\pi}_2\ell) = \langle \overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle \wedge \langle \overline{\pi}_1\ell\overline{\pi}_2\ell \xrightarrow{\mathtt{B} = \rho_{\mathtt{tt}}} \mathrm{at}[\![\mathtt{S}_b]\!],\ \overline{\pi}_3\rangle \in \widehat{\mathcal{S}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_b]\!]\}$$[6]

[5] If $\dot{\gamma}^i_{\mathbb{F}}(\dot{\varnothing}) = \varnothing$ then this case is $\varnothing$ when $\overline{\rho}_{\mathtt{ff}} = \dot{\varnothing}$.

[6] If $\dot{\gamma}^i_{\mathbb{F}}(\dot{\varnothing}) = \varnothing$ then this case is $\varnothing$ when $\overline{\rho}_{\mathtt{tt}} = \dot{\varnothing}$.

Proof I

- We let $\boldsymbol{\mathcal{F}}^*_{\mathbb{V}}$ be $\boldsymbol{\mathcal{F}}^*$ as defined in (17.4) for $\mathbb{V} = \mathbb{Z}$ generalized to $\mathbb{V} = \mathbb{R}$ and $\mathbb{V} = \mathbb{F}$
- The proof is based on Theorem 18.19
- Assuming that

$$\mathring{\alpha}^i_{\mathbb{F}}(X) \mathrel{\mathring{\mathbb{E}}^i} \overline{X} \text{ and } (32.32)$$

  we must prove that

$$\mathring{\alpha}^i_{\mathbb{F}}(\boldsymbol{\mathcal{F}}^*_{\mathbb{V}}[\![\texttt{while}^{\,\ell}\ \texttt{(B)}\ \mathtt{S}_b]\!]\ X) \mathrel{\mathring{\mathbb{E}}^i} \boldsymbol{\mathcal{F}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\,\ell}\ \texttt{(B)}\ \mathtt{S}_b]\!]\ \overline{X}$$

  to conclude that

$$\mathring{\alpha}^i_{\mathbb{F}}(\mathrm{lfp}^{\subseteq}\ \boldsymbol{\mathcal{F}}^*_{\mathbb{R}}[\![\texttt{while}^{\,\ell}\ \texttt{(B)}\ \mathtt{S}_b]\!]) \mathrel{\mathring{\mathbb{E}}^i} \mathrm{lfp}^{\dot{\subseteq}}\ \boldsymbol{\mathcal{F}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}^{\,\ell}\ \texttt{(B)}\ \mathtt{S}_b]\!]$$

- We have complete lattices hence CPOs. $\boldsymbol{\mathcal{F}}^*_{\mathbb{R}}$ does not preserves joins but is continuous.
- We define $\mathcal{I}$ in Theorem 18.19 by assuming that iterates X and $\overline{X}$ satisfy the induction hypothesis (32.32), which is trivially satisfied by the first iterates $\varnothing$

Proof II

$$
\begin{aligned}
&\mathring{\alpha}^i_{\mathbb{F}}(\boldsymbol{\mathcal{F}}^*_{\mathbb{V}}[\![\texttt{while}^{\,\ell}\ \texttt{(B)}\ \mathsf{S}_b]\!]\ X)\\
=\ &\mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi_1{}^{\ell},\ {}^{\ell}\rangle\} \cup \{\langle \pi_1{}^{\ell'},\ {}^{\ell'}\pi_2{}^{\ell'} \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'})} \mathrm{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_1{}^{\ell'},\ {}^{\ell'}\pi_2{}^{\ell'}\rangle \in X \wedge\\
&\boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'}) = \mathrm{ff} \wedge {}^{\ell'} = {}^{\ell}\} \cup \{\langle \pi_1{}^{\ell'},\ {}^{\ell'}\pi_2{}^{\ell'} \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'})} \mathrm{at}[\![\mathsf{S}_b]\!] \frown \pi_3\rangle \mid \langle \pi_1{}^{\ell'},\\
&{}^{\ell'}\pi_2{}^{\ell'}\rangle \in X \wedge \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'}) = \mathrm{tt} \wedge \langle \pi_1{}^{\ell'}\pi_2{}^{\ell'} \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'})} \mathrm{at}[\![\mathsf{S}_b]\!],\ \pi_3\rangle \in\\
&\boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \wedge {}^{\ell'} = {}^{\ell}\}) \qquad \text{(def (17.4) of } \boldsymbol{\mathcal{F}}^*_{\mathbb{V}}[\![\texttt{while}^{\,\ell}\ \texttt{(B)}\ \mathsf{S}_b]\!] \text{ and Section } \mathbf{32.5.5})\\
=\ &\mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi_1{}^{\ell},\ {}^{\ell}\rangle\}) \cup \mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi_1{}^{\ell'},\ {}^{\ell'}\pi_2{}^{\ell'} \xrightarrow{\neg(\mathsf{B}) = \boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'})} \mathrm{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_1{}^{\ell'},\ {}^{\ell'}\pi_2{}^{\ell'}\rangle \in X \wedge\\
&\boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'}) = \mathrm{ff} \wedge {}^{\ell'} = {}^{\ell}\}) \cup \mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi_1{}^{\ell'},\ {}^{\ell'}\pi_2{}^{\ell'} \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'})} \mathrm{at}[\![\mathsf{S}_b]\!] \frown \pi_3\rangle \mid \langle \pi_1{}^{\ell'},\\
&{}^{\ell'}\pi_2{}^{\ell'}\rangle \in X \wedge \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'}) = \mathrm{tt} \wedge \langle \pi_1{}^{\ell'}\pi_2{}^{\ell'} \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^{\ell'}\pi_2{}^{\ell'})} \mathrm{at}[\![\mathsf{S}_b]\!],\ \pi_3\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \wedge\\
&{}^{\ell'} = {}^{\ell}\}) \qquad \text{(join preservation in the Galois connection (32.25))}
\end{aligned}
$$

The first term has already been handled in the case of a conditional statement $\texttt{if}^{\,\ell}\ \texttt{(B)}\ \mathsf{S}_t$.

Proof III

This is also the case for the second term, but for $\langle \pi_1 \ell', \ell' \pi_2 \ell' \rangle \in X$ handled as in the third term below. For this third term (simplified with $\ell' = \ell$), we have

$$\dot{\alpha}^i_{\mathbb{F}}(\{\langle \pi_1\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1\ell\pi_2\ell)} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3\rangle \mid \langle \pi_1\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1\ell\pi_2\ell) =$$
$$\mathtt{tt} \wedge \langle \pi_1\ell\pi_2\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1\ell\pi_2\ell)} \mathsf{at}[\![\mathsf{S}_b]\!],\ \pi_3\rangle \in \mathscr{S}^*[\![\mathsf{S}_b]\!]\})$$
$$= \{\langle \vec{\alpha}^i_{\mathbb{F}}(\pi_1\ell),\ \vec{\alpha}^i_{\mathbb{F}}(\ell\pi_2\ell) \xrightarrow{\mathsf{B} = \dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi_1\ell\pi_2\ell))} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \vec{\alpha}^i_{\mathbb{F}}(\pi_3)\rangle \mid \langle \pi_1\ell,\ \ell\pi_2\ell\rangle \in X \wedge$$
$$\mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1\ell\pi_2\ell) = \mathtt{tt} \wedge \langle \pi_1\ell\pi_2\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1\ell\pi_2\ell)} \mathsf{at}[\![\mathsf{S}_b]\!],\ \pi_3\rangle \in \mathscr{S}^*[\![\mathsf{S}_b]\!]\}$$
(def. (32.14) of $\mathring{\alpha}^i_{\mathbb{F}}$)

$$\mathring{\mathbb{E}}^i \{\langle \overline{\pi}_1\ell,\ \ell\overline{\pi}_2\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \overline{\pi}_3\rangle \mid \langle \overline{\pi}_1\ell,\ \ell\overline{\pi}_2\ell\rangle \in \overline{X} \wedge \exists \overline{\rho}_{\mathtt{ff}}\ .\ \mathscr{B}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}_1\ell\overline{\pi}_2\ell) = \langle \overline{\rho}_{\mathtt{tt}},$$
$$\overline{\rho}_{\mathtt{ff}}\rangle \wedge \langle \overline{\pi}_1\ell\overline{\pi}_2\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \overline{\pi}_3\rangle \in \widehat{\mathscr{S}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathsf{S}_b]\!]\}$$
(By def. (32.27) of $\mathring{\mathbb{E}}^i$, we must find an interval execution *s.t.* $\langle \vec{\alpha}^i_{\mathbb{F}}(\pi_1\ell),$
$\vec{\alpha}^i_{\mathbb{F}}(\ell\pi_2\ell) \xrightarrow{\mathsf{B} = \dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi_1\ell\pi_2\ell))} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \vec{\alpha}^i_{\mathbb{F}}(\pi_3)\rangle \ddot{\mathbb{E}}^i \langle \overline{\pi}_1\ell, \ell\overline{\pi}_2\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \overline{\pi}_3\rangle$

Proof IV

The control abstraction is the same.

We can choose $\overline{\pi}_1{}^\ell = \vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell)$ so that, by ind. hyp. (32.32) and $\langle \pi_1{}^\ell, {}^\ell\pi_2{}^\ell \rangle \in X$, $\exists \overline{\pi}' \,.\, \langle \overline{\pi}_1{}^\ell, \overline{\pi}' \rangle \in \overline{X} \wedge \vec{\alpha}^i_{\mathbb{F}}({}^\ell\pi_2{}^\ell) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}'$. Therefore $\overline{\pi}'$ has the form $\overline{\pi}' = {}^\ell\overline{\pi}_2{}^\ell$ and so $\langle \overline{\pi}_1{}^\ell, {}^\ell\overline{\pi}_2{}^\ell \rangle \in \overline{X}$ with $\vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell\pi_2{}^\ell) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}_1{}^\ell\overline{\pi}_2{}^\ell$.

$\mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1{}^\ell\pi_2{}^\ell) = \mathtt{tt}$, $\langle \overline{\rho}^1_{\mathtt{tt}}, \overline{\rho}^1_{\mathtt{ff}} \rangle = \mathscr{B}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell\pi_2{}^\ell))$ and (32.18) imply that $\dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi_1{}^\ell\pi_2{}^\ell)) \mathrel{\dot{\sqsubseteq}^i} \overline{\rho}^1_{\mathtt{tt}}$.

$\mathscr{B}^i_{\mathbb{F}}[\![\mathsf{B}]\!]$ increasing, $\vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell\pi_2{}^\ell) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}_1{}^\ell\overline{\pi}_2{}^\ell$ and so $\boldsymbol{\varrho}(\vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell\pi_2{}^\ell)) \mathrel{\dot{\sqsubseteq}^i} \boldsymbol{\varrho}(\overline{\pi}_1{}^\ell\overline{\pi}_2{}^\ell)$ implies that $\langle \overline{\rho}_{\mathtt{tt}}, \overline{\rho}_{\mathtt{ff}} \rangle = \mathscr{B}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}_1{}^\ell\overline{\pi}_2{}^\ell)$ has $\overline{\rho}^1_{\mathtt{tt}} \mathrel{\dot{\sqsubseteq}^i} \overline{\rho}_{\mathtt{tt}}$

By transitivity, $\dot{\alpha}^i_{\mathbb{F}}(\boldsymbol{\varrho}(\pi_1{}^\ell\pi_2{}^\ell)) \mathrel{\dot{\sqsubseteq}^i} \overline{\rho}_{\mathtt{tt}}$.

It follows that $\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi_1{}^\ell, {}^\ell\pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell\pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!] \rangle) \mathrel{\ddot{\sqsubseteq}^i} \langle \overline{\pi}_1{}^\ell, {}^\ell\overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!] \rangle$
and therefore $\vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell\pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell\pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!]) \mathrel{\vec{\sqsubseteq}^i} \overline{\pi}_1{}^\ell\overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathtt{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!]$

Proof V

By $\langle \pi_1{}^\ell \pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell \pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!],\ \pi_3\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]$,
$\vec{\alpha}^i_{\mathbb{F}}(\pi_1{}^\ell \pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell \pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!]) \vec{\sqsubseteq}^i \overline{\pi}_1{}^\ell \overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathsf{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!]$ and ind. hyp. (32.32), there exists $\overline{\pi}_3$ such that $\vec{\alpha}^i_{\mathbb{F}}(\pi_3) \vec{\sqsubseteq}^i \overline{\pi}_3$ and $\langle \overline{\pi}_1{}^\ell \overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathsf{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!],\ \overline{\pi}_3\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathsf{S}_b]\!]$.

Therefore $\ddot{\alpha}^i_{\mathbb{F}}(\langle \pi_1{}^\ell,\ {}^\ell\pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell \pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!] \frown \pi_3\rangle) \ddot{\sqsubseteq}^i \langle \overline{\pi}_1{}^\ell,\ {}^\ell\overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathsf{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!] \frown \overline{\pi}_3\rangle$.

We conclude that

$\mathring{\alpha}^i_{\mathbb{F}}(\{\langle \pi_1{}^\ell,\ {}^\ell\pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell \pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!] \frown \pi_3\rangle \mid \langle \pi_1{}^\ell,\ {}^\ell\pi_2{}^\ell\rangle \in X \wedge \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_1{}^\ell \pi_2{}^\ell) =$
$\mathsf{tt} \wedge \langle \pi_1{}^\ell \pi_2{}^\ell \xrightarrow{\mathsf{B} = \boldsymbol{\varrho}(\pi_1{}^\ell \pi_2{}^\ell)} \mathrm{at}[\![\mathsf{S}_b]\!],\ \pi_3\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]\})$
$\mathring{\sqsubseteq}^i \{\langle \overline{\pi}_1{}^\ell,\ {}^\ell\overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathsf{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!] \frown \overline{\pi}_3\rangle \mid \langle \overline{\pi}_1{}^\ell,\ {}^\ell\overline{\pi}_2{}^\ell\rangle \in \overline{X} \wedge \exists \overline{\rho}_{\mathsf{ff}}\ .\ \boldsymbol{\mathcal{B}}^i_{\mathbb{F}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\overline{\pi}_1{}^\ell \overline{\pi}_2{}^\ell) = \langle \overline{\rho}_{\mathsf{tt}},$
$\overline{\rho}_{\mathsf{ff}}\rangle \wedge \langle \overline{\pi}_1{}^\ell \overline{\pi}_2{}^\ell \xrightarrow{\mathsf{B} = \overline{\rho}_{\mathsf{tt}}} \mathrm{at}[\![\mathsf{S}_b]\!],\ \overline{\pi}_3\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathsf{S}_b]\!]\}$

Proof VI

Since the above terms involves only computations in $\mathbb{S}_{\mathbb{P}^i}$ and none in $\mathbb{S}_{\mathbb{V}}$ and grouping all cases, we can define

$$\boldsymbol{\mathcal{F}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]\,\overline{X} \triangleq \{\langle\overline{\pi}^{\ell},\ \ell\rangle \mid \overline{\pi}^{\ell} \in \mathbb{T}^{+}_{\mathbb{P}^i_{\mathbb{R}}}\} \tag{32.34}$$

$$\cup\,\{\langle\overline{\pi}^{\ell},\ \ell \xrightarrow{\neg(\mathtt{B}) = \overline{\rho}_{\mathtt{ff}}} \mathsf{after}[\![\mathtt{S}]\!]\rangle \mid \langle\overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell}\rangle \in \overline{X} \wedge \exists\overline{\rho}_{\mathtt{tt}}\ .\ \boldsymbol{\mathcal{B}}^{i}_{\mathbb{F}}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\overline{\pi}^{\ell}) = \langle\overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle\}$$

$$\cup\,\{\langle\overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell} \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathtt{S}_b]\!] \frown \overline{\pi}_3\rangle \mid \langle\overline{\pi}_1{}^{\ell},\ {}^{\ell}\overline{\pi}_2{}^{\ell}\rangle \in \overline{X} \wedge \exists\overline{\rho}_{\mathtt{ff}}\ .\ \boldsymbol{\mathcal{B}}^{i}_{\mathbb{F}}[\![\mathtt{B}]\!]\overline{\rho} = \langle\overline{\rho}_{\mathtt{tt}},\ \overline{\rho}_{\mathtt{ff}}\rangle$$

$$\wedge\ \langle\overline{\pi}_1{}^{\ell}\overline{\pi}_2{}^{\ell} \xrightarrow{\mathtt{B} = \overline{\rho}_{\mathtt{tt}}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \overline{\pi}_3\rangle \in \widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\mathtt{S}_b]\!]\}$$

so that we proved that $\mathring{\alpha}^{i}_{\mathbb{F}}(X)\ \mathring{\mathbb{E}}^{i}\ \overline{X}$ implies $\mathring{\alpha}^{i}_{\mathbb{F}}(\boldsymbol{\mathcal{F}}^{*}_{\mathbb{R}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]\ X)\ \mathring{\mathbb{E}}^{i}$ $\boldsymbol{\mathcal{F}}^{*}_{\mathbb{P}^i_{\mathbb{F}}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]\,\overline{X}$.

Proof VII

We have to show that the next iterate $\boldsymbol{\mathcal{F}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]\ X$ satisfies (32.32), which is trivial for the first two terms. For the third term this follows from the induction hypothesis. It follows that

$$
\begin{array}{rll}
 & \mathring{\alpha}^{i}_{\mathbb{F}}(\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{V}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]) & (32.35)\\
= & \mathring{\alpha}^{i}_{\mathbb{F}}(\mathrm{lfp}^{\subseteq}\,\boldsymbol{\mathcal{F}}^{*}_{\mathbb{R}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]) & \text{by (17.4)}\\
\mathrel{\mathring{\sqsubseteq}}^{i} & \mathrm{lfp}^{\dot{\subseteq}}\,\boldsymbol{\mathcal{F}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!] & \text{by Theorem 18.19}\\
\triangleq & \widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!] & \text{def. (32.34)}
\end{array}
$$

It remains to show that $\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{P}^{i}_{\mathbb{F}}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]$ satisfies (32.32). We have shown that it holds for all fixpoint iterates. Moreover, it is trivially preserved by trace set union. □

See the other proofs in the book.

Home work

Read Ch. **32** "Dynamic interval analysis" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you