SOAP 2021
10th ACM SIGPLAN International Workshop on the State of the Art in Program Analysis

Dynamic abstract interpretation

Patrick Cousot

NYU, New York

pcousot@cs.nyu.edu   cs.nyu.edu/~pcousot

Tuesday, June 22th, 2021

Interval arithmetics

- In scientific computing a real number is represented by a float (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 arithmetic" to put bounds on rounding errors in floating point computations.
- This guarantees that the uncertain real computation is between floating point bounds
- We show that "interval arithmetic" is a sound abstract interpretation of the program semantics (on reals).
- Maybe the first dynamic analysis of programs.

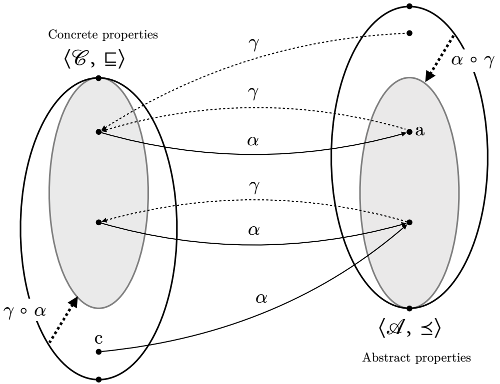
en.wikipedia.org/wiki/Interval_arithmetic

Abstract interpretation

Interval abstraction

concrete property	abstraction	abstract property	concretization	concrete overapproximation
$\{1.0/9.0, 1.0/7.0, 1.0/3.0\}$	$\longrightarrow\alpha\rightarrow$	$[0.11110, 0.33334]$	$\longrightarrow\gamma\rightarrow$	$\{0.11110, \ldots, 1.0/9.0, \ldots, 0.14286\cdots,$ $\ldots, 1.0/7.0, \ldots, 1.0/3.0, \ldots, 0.33334\}$
$\in \wp(\mathbb{R})$		$\in \mathbb{F}\times\mathbb{F}$		$\in \wp(\mathbb{R})$

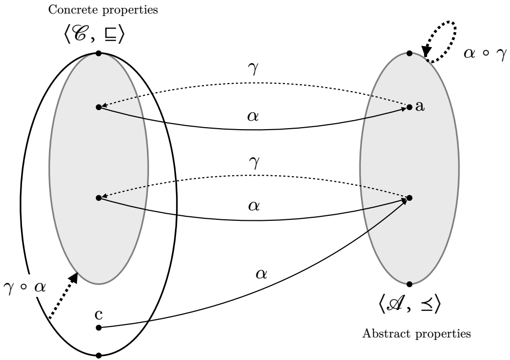
Galois connection



$$\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preceq \rangle$$

$$\alpha(c) \preceq a \Leftrightarrow c \sqsubseteq \gamma(a)$$

Galois retraction/insertion



$$\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preceq \rangle$$

$\alpha(c) \preceq a \Leftrightarrow c \sqsubseteq \gamma(a) \wedge \alpha$ surjective

Interval abstraction

Values

- Programs compute on values $\mathbb{V}$.
- Values $\mathbb{V}$ can be the set of
  - $\mathbb{R}$ of reals.
  - $\mathbb{F}$ of floats [1]
  - $\mathbb{P}^i$ of float intervals

  For simplicity, we assume that execution stops in case of error (e.g. when dividing by zero or returning NaN).

Properties

- Properties are sets of values e.g. $\{x \in \mathbb{V} \mid x > 0\}$ is "to be positive"
- A semantics is the strongest property of executions

[1] We include ±infinity but exclude NaN, -0, $+0$ for simplicity of the presentation, not hard to handle.

Interval abstraction

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

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

Example 1 In interval arithmetics, a real is abstracted by the pair of enclosing floats. This is also the abstraction of the set of reals between these two floats □

Abstract domain of numerical intervals

- We let the abstract domain of float intervals be

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

  where the empty interval $\perp^i = \varnothing$ can be encoded by any $[\underline{x}, \overline{x}]$ with $\overline{x} < \underline{x}$ (e.g. normalized to $[\infty, -\infty]$).
- The intervals $[-\infty, -\infty] \notin \mathbb{P}^i$ and $[\infty, \infty] \notin \mathbb{P}^i$ are excluded.

Abstract domain of numerical intervals

- We let the abstract domain of float intervals be

$$\begin{array}{rcl}\mathbb{P}^i & \triangleq & \{\varnothing\} \cup \{[\underline{x}, \overline{x}] \mid \underline{x}, \overline{x} \in \mathbb{F} \setminus \{-\infty, \infty\} \wedge \underline{x} \leqslant \overline{x}\} \\ & \cup & \{[-\infty, \overline{x}] \mid \overline{x} \in \mathbb{F} \setminus \{-\infty\}\} \cup \{[\underline{x}, \infty] \mid \underline{x} \in \mathbb{F} \setminus \{\infty\}\}\end{array}$$

  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 $[-\infty, -\infty] \notin \mathbb{P}^i$ and $[\infty, \infty] \notin \mathbb{P}^i$ are excluded.

- The partial order $\sqsubseteq^i$ on $\mathbb{P}^i$ 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 $\underline{y} \leqslant \underline{x} \leqslant \overline{x} \leqslant \overline{y}$.

- This is a complete lattice $\langle \mathbb{P}^i,\ \sqsubseteq^i,\ \varnothing,\ [-\infty, +\infty],\ \bigsqcap^i,\ \bigsqcup^i \rangle$

Abstract domain of numerical intervals

- We let the abstract domain of float intervals be

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

  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 $[-\infty, -\infty] \notin \mathbb{P}^i$ and $[\infty, \infty] \notin \mathbb{P}^i$ are excluded.
- The partial order $\sqsubseteq^i$ on $\mathbb{P}^i$ 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 $\underline{y} \leqslant \underline{x} \leqslant \overline{x} \leqslant \overline{y}$.
- This is a complete lattice $\langle \mathbb{P}^i,\ \sqsubseteq^i,\ \varnothing,\ [-\infty, +\infty],\ \sqcap^i,\ \sqcup^i \rangle$
- We have the Galois retraction

$$\langle \wp(\mathbb{R}),\ \subseteq \rangle \xrightleftharpoons[\alpha_i]{\gamma_i} \langle \mathbb{P}^i,\ \sqsubseteq^i \rangle \qquad (2)$$

Soundness

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

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

Soundness

- Given parameters $x \in [\underline{x}, \overline{x}]$, $y \in [\underline{y}, \overline{y}]$, … the interval computation of a function $f \in \mathbb{R}^n \longrightarrow \mathbb{R}$ 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! α_i is the best/most precise abstraction.

Soundness

- Given parameters $x \in [\underline{x}, \overline{x}]$, $y \in [\underline{y}, \overline{y}]$, … the interval computation of a function $f \in \mathbb{R}^n \longrightarrow \mathbb{R}$ 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! α_i is the best/most precise abstraction.

- Formally, the soundness condition is

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

Syntax and trace semantics of programs

Syntax

$\mathtt{x}, \mathtt{y}, \ldots \in \mathbb{V}$		variable ($\mathbb{V}$ not empty)
$\mathtt{A} \in \mathbb{A}$	$::= \mathtt{0.1} \mid \mathtt{x} \mid \mathtt{A}_1 - \mathtt{A}_2$	arithmetic expression
$\mathtt{B} \in \mathbb{B}$	$::= \mathtt{A}_1 < \mathtt{A}_2 \mid \mathtt{B}_1\ \mathtt{nand}\ \mathtt{B}_2$	boolean expression
$\mathtt{S} \in \mathbb{S}$	$::=$	statement
	$\mathtt{x} = \mathtt{A}\ ;$	assignment
	$\mid\ ;$	skip
	$\mid\ \mathtt{\textbf{if}}\ (\mathtt{B})\ \mathtt{S} \mid \mathtt{\textbf{if}}\ (\mathtt{B})\ \mathtt{S}\ \mathtt{\textbf{else}}\ \mathtt{S}$	conditionals
	$\mid\ \mathtt{\textbf{while}}\ (\mathtt{B})\ \mathtt{S} \mid \mathtt{\textbf{break}}\ ;$	iteration and break
	$\mid\ \{\ \mathtt{Sl}\ \}$	compound statement
$\mathtt{Sl} \in \mathbb{Sl}$	$::= \mathtt{Sl}\ \mathtt{S} \mid \epsilon$	statement list
$\mathtt{P} \in \mathbb{P}$	$::= \mathtt{Sl}$	program
$\mathtt{S} \in \mathbb{Pc}$	$\triangleq \mathbb{S} \cup \mathbb{Sl} \cup \mathbb{P}$	program component

The float constant $\mathtt{0.1}$ is $0.000(1100)^\infty$ in binary so has no exact finite binary representation. It is approximated as $0.100000001490116119384765625 00\ldots$.

Program labelling

Unique labelling to designate (sets of) program points $\ell \in \mathbb{L}$:

$\mathsf{at}[\![\mathsf{S}]\!]$	the program point at which execution of S starts;
$\mathsf{after}[\![\mathsf{S}]\!]$	the program exit point after S, at which execution of S is supposed to normally terminate, if ever;
$\mathsf{escape}[\![\mathsf{S}]\!]$	a boolean indicating whether or not the program component S contains a **break ;** statement escaping out of that component S;
$\mathsf{break\text{-}to}[\![\mathsf{S}]\!]$	the program point at which execution of the program component S goes to when a **break ;** statement escapes out of that component S;
$\mathsf{breaks\text{-}of}[\![\mathsf{S}]\!]$	the set of labels of all **break ;** statements that can escape out of S

Example of program labelling

$$\overbrace{\texttt{while}\ \ell_0\ (\cdots)\ \{\ \overbrace{\ell_1\ \overbrace{\cdots}^{\mathsf{S}_1}\ \ell_2\ \overbrace{\texttt{break}\ ;}^{\mathsf{S}_2}\cdots\ \ell_3\ \overbrace{\texttt{break}\ ;}^{\mathsf{S}_3}\ \overbrace{\cdots}^{\mathsf{S}_4}}^{\mathsf{S}_b}\ \}}^{\mathsf{S}}\ \ell_5\ \overbrace{\cdots}^{\mathsf{S}_5}$$

$$\begin{array}{lllllll}
\ell_0 & = & \mathsf{at}[\![\mathsf{S}]\!] & = & \mathsf{after}[\![\mathsf{S}_4]\!] \\
\ell_1 & = & \mathsf{at}[\![\mathsf{S}_1]\!] & = & \mathsf{at}[\![\mathsf{S}_b]\!] \\
\ell_2 & = & \mathsf{at}[\![\mathsf{S}_2]\!] & = & \mathsf{after}[\![\mathsf{S}_1]\!] \\
\ell_3 & = & \mathsf{at}[\![\mathsf{S}_3]\!] \\
\ell_5 & = & \mathsf{at}[\![\mathsf{S}_5]\!] & = & \mathsf{break\text{-}to}[\![\mathsf{S}_b]\!] & = & \mathsf{after}[\![\mathsf{S}]\!]
\end{array}$$

$$\mathsf{escape}[\![\mathsf{S}_b]\!] = tt \quad \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] = \{\ell_2, \ell_3\},$$

$$\mathsf{escape}[\![\mathsf{S}]\!] = ff,$$

$$\mathsf{in}[\![\mathsf{S}_b]\!] = \{\ell_1, \ldots, \ell_2, \ldots, \ell_3, \ldots\}$$

$$\mathsf{in}[\![\mathsf{S}]\!] = \mathsf{labx}[\![\mathsf{S}_b]\!] = \{\ell_0, \ell_1, \ldots, \ell_2, \ldots, \ell_3, \ldots\},$$

$$\mathsf{labx}[\![\mathsf{S}]\!] = \{\ell_0, \ell_1, \ldots, \ell_2, \ldots, \ell_3, \ldots, \ell_5\}$$

Prefix traces

- Program label: $\ell \in \mathbb{L}$ (locates next step to be executed in the program)
- Environment: $\rho \in \mathbb{E}\mathrm{v}_{\mathbb{V}} \triangleq \mathbb{V} \to \mathbb{V}$ assigns values $\rho(\mathrm{x}) \in \mathbb{V}$ to variables $\mathrm{x} \in \mathbb{V}$.
- State: $\langle \ell,\ \rho \rangle \in \mathbb{S}_{\mathbb{V}} \triangleq (\mathbb{L} \times \mathbb{E}\mathrm{v}_{\mathbb{V}})$
- Trace: finite or infinite sequence $\pi \in \mathbb{S}_{\mathbb{V}}^{+\infty}$ of states
- Example: $\langle \ell_1,\ \{\mathrm{x} \to 1\}\rangle\langle \ell_2,\ \{\mathrm{x} \to 2\}\rangle\langle \ell_4,\ \{\mathrm{x} \to 2\}\rangle$
- Trace concatenation: $\frown$

$$
\begin{array}{rcll}
\pi_1\sigma_1 \frown \sigma_2\pi_2 & & & \text{undefined if } \sigma_1 \neq \sigma_2 \\
\pi_1 \frown \sigma_2\pi_2 & \triangleq & \pi_1 & \text{if } \pi_1 \in \mathbb{S}_{\mathbb{V}}^{+} \text{ is infinite} \\
\pi_1\sigma_1 \frown \sigma_1\pi_2 & \triangleq & \pi_1\sigma_1\pi_2 & \text{if } \pi_1 \in \mathbb{T}^{+} \text{ is finite}
\end{array}
$$

- In pattern matching, we sometimes need the empty trace $\ni$. For example if $\sigma\pi\sigma' = \sigma$ then $\pi = \ni$ and $\sigma = \sigma'$.

Evaluation of expressions

- Evaluation of an arithmetic expression (parameterized by $\mathbb{V} = \mathbb{R}$ or $\mathbb{V} = \mathbb{F}$, later intervals)

$$
\begin{aligned}
\mathscr{A}_{\mathbb{V}}[\![\mathtt{0.1}]\!]\rho &\triangleq 0.1_{\mathbb{V}} \\
\mathscr{A}_{\mathbb{V}}[\![\mathsf{x}]\!]\rho &\triangleq \rho(\mathsf{x}) \\
\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1 - \mathsf{A}_2]\!]\rho &\triangleq \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho -_{\mathbb{V}} \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho
\end{aligned}
\tag{1}
$$

- 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.

Evaluation of expressions

- Evaluation of an arithmetic expression (parameterized by $\mathbb{V} = \mathbb{R}$ or $\mathbb{V} = \mathbb{F}$, later intervals)

$$
\begin{aligned}
\mathscr{A}_{\mathbb{V}}[\![\texttt{0.1}]\!]\rho &\triangleq 0.1_{\mathbb{V}} \\
\mathscr{A}_{\mathbb{V}}[\![\mathsf{x}]\!]\rho &\triangleq \rho(\mathsf{x}) \\
\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1 - \mathsf{A}_2]\!]\rho &\triangleq \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho -_{\mathbb{V}} \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho
\end{aligned}
\tag{1}
$$

- 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.
- Evaluation of a Boolean expression ($\mathbb{B} \triangleq \{\mathrm{tt}, \mathrm{ff}\}$):

$$
\begin{aligned}
\mathscr{B}_{\mathbb{V}}[\![\mathsf{A}_1 < \mathsf{A}_2]\!]\rho &\triangleq \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho < \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho \\
\mathscr{B}_{\mathbb{V}}[\![\mathsf{B}_1 \ \mathsf{nand}\ \mathsf{B}_2]\!]\rho &\triangleq \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}_1]\!]\rho \uparrow \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}_2]\!]\rho
\end{aligned}
\tag{4}
$$

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

Prefix trace semantics

- A prefix trace describes the beginning of a computation
- Assignment $\mathsf{S} ::= {}^{\ell}\ \mathsf{x} = \mathsf{A}\ ;$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$
\begin{aligned}
\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!] \;=\;& \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \\
& \{\langle \ell,\ \rho\rangle \langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho[\mathsf{x} \leftarrow \boldsymbol{\mathcal{A}}_{\mathbb{V}}[\![\mathsf{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}
\end{aligned} \tag{2}
$$

Prefix trace semantics (cont'd)

- Break statement $\mathsf{S} ::= \ell\ \mathtt{break}\ ;$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$\begin{aligned}\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!] \triangleq\ & \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \\ & \{\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}\end{aligned} \tag{3}$$

Prefix trace semantics (cont'd)

- Conditional statement $\mathsf{S} ::= \mathtt{if}\ \ell\ (\mathsf{B})\ \mathsf{S}_t$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$
\begin{aligned}
\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!] \triangleq\ & \{\langle\ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \\
& \cup \{\langle\ell,\ \rho\rangle\langle\mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\rho = \mathit{ff}\} \\
& \cup \{\langle\ell,\ \rho\rangle\langle\mathsf{at}[\![\mathsf{S}_t]\!],\ \rho\rangle\pi \mid \mathcal{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\rho = \mathit{tt} \wedge \langle\mathsf{at}[\![\mathsf{S}_t]\!],\ \rho\rangle\pi \in \boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}_t]\!]\}
\end{aligned}
\tag{5}
$$

- If the conditional statement S is inside an iteration statement, and S_t has a break, the execution goes on at the $\mathsf{break\text{-}to}[\![\mathsf{S}]\!]$ after the iteration.

Prefix trace semantics (cont'd)

- Statement list $\texttt{Sl} ::= \texttt{Sl}'\ \texttt{S}$ (where $\mathsf{at}[\![\texttt{S}]\!] = \mathsf{after}[\![\texttt{Sl}']\!]$)

$$\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{Sl}]\!] \triangleq \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{Sl}']\!] \cup \qquad (7)$$
$$\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{Sl}']\!] \frown \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{S}]\!] \qquad (3)$$

$$\boldsymbol{\mathcal{S}} \frown \boldsymbol{\mathcal{S}}' \triangleq \{\pi \frown \pi' \mid \pi \in \boldsymbol{\mathcal{S}} \wedge \pi' \in \boldsymbol{\mathcal{S}}' \wedge \pi \frown \pi' \text{ is well-defined}\}$$

- $\pi' \in \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{S}]\!]$ starts $\mathsf{at}[\![\texttt{S}]\!] = \mathsf{after}[\![\texttt{Sl}']\!]$ so, by def. $\frown$, the trace $\pi \in \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{Sl}']\!]$ must terminate to be able to go on with $\texttt{S}$.

Prefix trace semantics (cont'd)

- Empty statement list $\texttt{Sl} ::= \epsilon$ (where $\mathsf{at}[\![\texttt{Sl}]\!] \triangleq \mathsf{after}[\![\texttt{Sl}]\!]$)

$$\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\texttt{Sl}]\!] \triangleq \{\langle \mathsf{at}[\![\texttt{Sl}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathrm{v}\}$$

Prefix trace semantics (cont'd)

- Iteration statement $\mathsf{S} ::= \mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

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

$$\begin{aligned}
\boldsymbol{\mathcal{F}}^*_{\mathbb{V}}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]\ X \quad &\triangleq \quad \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} && \text{(a)}\\
&\cup \big\{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\,\rho = \mathsf{ff} \wedge \ell' = \ell\big\} && \text{(b)}\\
&\cup \big\{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \boldsymbol{\mathcal{B}}_{\mathbb{V}}[\![\mathsf{B}]\!]\,\rho = \mathsf{tt} \wedge && \text{(c)}\\
&\qquad\qquad \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \in \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}_b]\!] \wedge \ell' = \ell\big\}
\end{aligned}$$

(a) either the execution observation stop $\mathsf{at}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] = \ell$, or

(b) after a number of iterations, control is back to ℓ, the test is false, and the loop is exited, or

(c) after a number of iterations, control is back to ℓ, the test is true, and the loop body is executed

(This includes the termination of the loop body $\mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] = \ell$)

Maximal trace semantics

- Maximal trace semantics

$$\boldsymbol{\mathcal{S}}^{+}_{\mathbb{V}}[\![\mathsf{S}]\!] \triangleq \{\pi\langle\ell,\ \rho\rangle \in \boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!] \mid (\ell = \mathsf{after}[\![\mathsf{S}]\!]) \vee (\mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell = \mathsf{break\text{-}to}[\![\mathsf{S}]\!])\}$$

$$\boldsymbol{\mathcal{S}}^{\infty}_{\mathbb{V}}[\![\mathsf{S}]\!] \triangleq \lim(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!])$$

- Limit

$$\lim \mathscr{T} \triangleq \{\pi \in \mathbb{T}^{\infty} \mid \forall n \in \mathbb{N} \,.\, \pi[0..n] \in \mathscr{T}\}.$$

Objective

Objective

- We have defined the value semantics $\mathcal{S}^*_{\mathbb{V}}$ of the language (its executions on reals are not implementable/too costly to implement[2])

[2] e.g. using Bill Gosper's exact algorithms for continued fraction arithmetic.

Objective

- We have defined the value semantics $\mathcal{S}^*_{\mathbb{V}}$ of the language (its executions on reals are not implementable/too costly to implement[2])

- Next, we define the interval abstraction $\mathring{\alpha}^{\mathbb{P}^i}$ of a value semantics (replacing reals by float intervals)

[2] e.g. using Bill Gosper's exact algorithms for continued fraction arithmetic.

Objective

- We have defined the value semantics $\mathcal{S}^*_{\mathbb{V}}$ of the language (its executions on reals are not implementable/too costly to implement[2])
- Next, we define the interval abstraction $\mathring{\alpha}^{\mathbb{P}^i}$ of a value semantics (replacing reals by float intervals)
- The best float interval semantics of the value semantics is $\mathring{\alpha}^{\mathbb{P}^i}(\mathcal{S}^*_{\mathbb{V}})$ (its executions on interval float abstractions of reals are not implementable)

[2] e.g. using Bill Gosper's exact algorithms for continued fraction arithmetic.

Objective

- We have defined the value semantics $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}$ of the language (its executions on reals are not implementable/too costly to implement[2])

- Next, we define the interval abstraction $\mathring{\alpha}^{\mathbb{P}^i}$ of a value semantics (replacing reals by float intervals)

- The best float interval semantics of the value semantics is $\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}})$ (its executions on interval float abstractions of reals are not implementable)

- We define a sound over-approximation partial order $\mathring{\sqsubseteq}^i$ of interval semantics (with larger intervals)

[2] e.g. using Bill Gosper's exact algorithms for continued fraction arithmetic.

Objective

- We have defined the value semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}$ of the language (its executions on reals are not implementable/too costly to implement[2])
- Next, we define the interval abstraction $\mathring{\alpha}^{\mathbb{P}^i}$ of a value semantics (replacing reals by float intervals)
- The best float interval semantics of the value semantics is $\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}})$ (its executions on interval float abstractions of reals are not implementable)
- We define a sound over-approximation partial order $\mathring{\sqsubseteq}^{i}$ of interval semantics (with larger intervals)
- Next, we calculate the interval semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}$ of the language (executions on float intervals)

[2] e.g. using Bill Gosper's exact algorithms for continued fraction arithmetic.

Objective

- We have defined the value semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}$ of the language (its executions on reals are not implementable/too costly to implement[2])
- Next, we define the interval abstraction $\mathring{\alpha}^{\mathbb{P}^i}$ of a value semantics (replacing reals by float intervals)
- The best float interval semantics of the value semantics is $\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}})$ (its executions on interval float abstractions of reals are not implementable)
- We define a sound over-approximation partial order $\mathring{\sqsubseteq}^{i}$ of interval semantics (with larger intervals)
- Next, we calculate the interval semantics $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}$ of the language (executions on float intervals)
- By construction $\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}) \mathrel{\mathring{\sqsubseteq}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}$, so the interval semantics is a sound abstraction of the value semantics

[2] e.g. using Bill Gosper's exact algorithms for continued fraction arithmetic.

Interval arithmetics

How real computations are performed?

- Floating point arithmetics: floating point number representing an uncertain real x

How real computations are performed?

- Floating point arithmetics: floating point number representing an uncertain real x
- Interval arithmetics: the computation is performed with the two ends of a float interval $[\underline{x}, \overline{x}]$ with $x \in [\underline{x}, \overline{x}]$.
- This is an abstraction of a trace semantics on reals

How real computations are performed?

- Floating point arithmetics: floating point number representing an uncertain real x
- Interval arithmetics: the computation is performed with the two ends of a float interval $[\underline{x}, \overline{x}]$ with $x \in [\underline{x}, \overline{x}]$.
- This is an abstraction of a trace semantics on reals
- Handling tests:
  - real computation: only one branch taken
  - float computation: only one branch taken, but could be the wrong one
  - interval computation: one or both alternatives taken (hence one real trace can be abstracted into interval several traces).

Constants

- If the program contains a constant c, its interval is $[c, c]$.
- However, the compilation may introduce an error i.e. 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

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

- 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 ∞.
- This implies that the computed value is always included in the concretization of the interval value.
- Interval arithmetic is imprecise does not identify different occurrences of the same variable.

Multiplication

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

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

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

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

Conditions

- Although when computing with $\mathbb{R}$ only one branch of a conditional will be taken, interval computation with $\mathbb{P}^i$ may have to take both.
- This gives, in the worst-case, an exponential number of cases to consider.

Conditions

- Although when computing with $\mathbb{R}$ only one branch of a conditional will be taken, interval computation with $\mathbb{P}^i$ 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.
- See e.g. `www.boost.org/doc/libs/1_74_0/libs/numeric/interval/doc/interval.htm` and `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).

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

Float interval abstraction

Float notations

- $\Lsh\!\| x$ (which can be $-\infty$) is the largest float smaller than or equal to $x \in \mathbb{R}$ (or $\Lsh\!\| x = x$ for $x \in \mathbb{F}$)
- $x \|\!\Rsh$ (which can be ∞) is the smallest float greater than or equal to $x \in \mathbb{R}$ (or $x \|\!\Rsh = x$ for $x \in \mathbb{F}$).
- $\Lsh\!| x$ is the largest floating-point number strictly less than $x \in \mathbb{F}$ (which can be $-\infty$)
- $x |\!\Rsh$ is the smallest floating-point number strictly larger than $x \in \mathbb{F}$ (which can be ∞).
- We assume

$$
\begin{array}{rcll}
\Lsh\!\| x -_{\mathbb{F}} y \|\!\Rsh & \leqslant & \Lsh\!\| (x -_{\mathbb{V}} y) & (\mathbb{V} \text{ is } \mathbb{R} \text{ or } \mathbb{F}) \quad (12) \\
x \|\!\Rsh -_{\mathbb{F}} \Lsh\!\| y & \geqslant & (x -_{\mathbb{V}} y) \|\!\Rsh & \\
(\mathrm{x} \in [\underline{x}, \overline{x}] \wedge \mathrm{y} \in [\underline{y}, \overline{y}] \wedge \mathrm{x} < \mathrm{y}) & \Rightarrow & (\mathrm{x} \in [\underline{x}, \min(\overline{x}, \overline{y})] \wedge \mathrm{y} \in [\max(\underline{x}, \underline{y}), \overline{y}]) & \quad (13)
\end{array}
$$

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

$$(\mathrm{x} \in [\underline{x}, \overline{x}] \wedge \mathrm{y} \in [\underline{y}, \overline{y}] \wedge \mathrm{x} < \mathrm{y}) \quad \Rightarrow \quad (\mathrm{x} \in [\underline{x}, \min(\overline{x}, \overline{y}\,\lceil\!\!\rightarrow))] \wedge \mathrm{y} \in [\max(\leftarrow\!\!\rceil\,\underline{x}, \underline{y}), \overline{y}]) \qquad (13.\mathrm{bis})$$

en.wikipedia.org/wiki/Pentium_FDIV_bug

Float interval abstraction

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

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

$$\langle \wp(\mathbb{S}^{+\infty}_{\mathbb{V}}),\ \subseteq\rangle \xleftarrow[\mathring{\alpha}^{\mathbb{P}^i}]{\mathring{\gamma}^{\mathbb{P}^i}} \langle \wp(\mathbb{S}^{+\infty}_{\mathbb{P}^i}),\ \subseteq\rangle \quad (15)$$

$\subseteq$ is correct by inadequate for approximation in the abstract

- Program: ℓ_1 x = x − x ; ℓ_2
- Concrete semantics:

$$\varPi = \{\langle \ell_1,\ \mathtt{x} = 0.1_{\mathbb{R}}\rangle\langle \ell_2,\ \mathtt{x} = 0.0_{\mathbb{R}}\rangle,\quad \langle \ell_1,\ \mathtt{x} = -0.1_{\mathbb{R}}\rangle\langle \ell_2,\ \mathtt{x} = 0.0_{\mathbb{R}}\rangle\}$$

- Sound abstract semantics on floats:

$$\begin{aligned}
\overline{\varPi}_1 &= \{\langle \ell_1,\ \mathtt{x} = [0.09, 0.11]\rangle\langle \ell_2,\ \mathtt{x} = [0.00, 0.00]\rangle, & \varPi \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\overline{\varPi}_1)\\
&\qquad \langle \ell_1,\ \mathtt{x} = [-0.11, -0.09]\rangle\langle \ell_2,\ \mathtt{x} = [0.00, 0.00]\rangle\} & \\
\overline{\varPi}_2 &= \{\langle \ell_1,\ \mathtt{x} = \underbrace{[-0.11, 0.11]}_{\text{input interval}}\rangle\langle \ell_2,\ \mathtt{x} = \underbrace{[-0.02, 0.20]}_{\text{interval arithmetic}}\rangle\} & \varPi \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\overline{\varPi}_2)
\end{aligned}$$

- $\overline{\varPi}_1$ and $\overline{\varPi}_2$ are <u>not</u> comparable as abstract elements of $\langle \wp(\mathbb{S}^{+\infty}_{\mathbb{P}^i}),\ \subseteq\rangle$
- So $\subseteq$ does not allow over approximating $\overline{\varPi}_1$ by $\overline{\varPi}_2$!

Sound over-approximation in the concrete

- Concrete semantics:

$$\Pi = \{\langle \ell_1,\ \mathtt{x} = 0.1_{\mathbb{R}}\rangle\langle \ell_2,\ \mathtt{x} = 0.0_{\mathbb{R}}\rangle,\quad \langle \ell_1,\ \mathtt{x} = -0.1_{\mathbb{R}}\rangle\langle \ell_2,\ \mathtt{x} = 0.0_{\mathbb{R}}\rangle\}$$

- Sound abstract semantics on floats:

$$\begin{array}{rcll}
\overline{\Pi}_1 & = & \{\langle \ell_1,\ \mathtt{x} = [0.09, 0.11]\rangle\langle \ell_2,\ \mathtt{x} = [0.00, 0.00]\rangle, & \Pi \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\overline{\Pi}_1) \\
 & & \quad \langle \ell_1,\ \mathtt{x} = [-0.11, -0.09]\rangle\langle \ell_2,\ \mathtt{x} = [0.00, 0.00]\rangle\} & \\
\overline{\Pi}_2 & = & \{\langle \ell_1,\ \mathtt{x} = \underbrace{[-0.11, 0.11]}_{\text{input interval}}\rangle\langle \ell_2,\ \mathtt{x} = \underbrace{[-0.02, 0.20]}_{\text{interval arithmetic}}\rangle\} & \Pi \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\overline{\Pi}_2)
\end{array}$$

- By comparison in the concrete, $\overline{\Pi}_1$ is more precise than $\overline{\Pi}_2$, written $\overline{\Pi}_1 \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}_2$

$$\begin{array}{rcl}
\overline{\Pi}_1 \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}_2 & \triangleq & \mathring{\gamma}^{\mathbb{P}^i}(\overline{\Pi}_1) \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\overline{\Pi}_2) \\
 & = & \forall \overline{\pi}_1 \in \overline{\Pi}_1 \;.\; \forall \pi \in \vec{\gamma}^{\mathbb{P}^i}(\overline{\pi}_1) \;.\; \exists \overline{\pi}_2 \in \overline{\Pi}_2 \;.\; \pi \in \vec{\gamma}^{\mathbb{P}^i}(\overline{\pi}_2)
\end{array} \tag{16}$$

Sound over-approximation in the abstract

- We express $\mathring{\sqsubseteq}^i$ in the abstract, without referring to te concretization $\vec{\gamma}^{\mathbb{P}^i}$
- We define $\overline{\Pi}\ \mathring{\sqsubseteq}^i\ \overline{\Pi}'$ 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.

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

Sound over-approximation in the abstract

- We express $\mathrel{\mathring{\sqsubseteq}}^i$ in the abstract, without referring to te concretization $\vec{\gamma}^{\mathbb{P}^i}$
- 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).
- $\mathrel{\mathring{\sqsubseteq}}^i$ is Hoare preorder [Winskel, 1983] on sets of traces.

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

Lemma 6 $(\overline{\Pi} \mathrel{\mathring{\sqsubseteq}}^i \overline{\Pi}') \Rightarrow (\overline{\Pi} \mathrel{\mathring{\sqsubseteq}}^i \overline{\Pi}')$. □

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

- Strictly weaker
- Example:

$$
\begin{aligned}
\overline{\Pi}_1 &= \{\langle \ell_1,\ \mathsf{x} = [0.0, 1.0]\rangle,\\
&\phantom{= \{}\langle \ell_1,\ \mathsf{x} = [1.0, 2.0]\rangle\}\\
\overline{\Pi}_2 &= \{\langle \ell_1,\ \mathsf{x} = [0.0, 0.5]\rangle,\\
&\phantom{= \{}\langle \ell_1,\ \mathsf{x} = [0.5, 2.0]\rangle\}
\end{aligned}
$$

- $\overline{\Pi}_1 \mathrel{\mathring{\sqsubseteq}^i} \overline{\Pi}_2$ (same concrete traces)
- $\overline{\Pi}_1 \mathrel{\mathring{\not\sqsubseteq}^i} \overline{\Pi}_2$ (no inclusion of abstract traces)
- $\overline{\Pi}_2 \mathrel{\mathring{\not\sqsubseteq}^i} \overline{\Pi}_1$

Soundness and calculational design

- Value (real/float) concrete semantics: $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!]$
- Interval abstract semantics: $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}[\![\mathsf{S}]\!]$
- Soundness: all value (real/float) traces are included in the interval traces:

$$
\begin{array}{lll}
 & \mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!]) \mathrel{\dot{\mathring{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}[\![\mathsf{S}]\!] & \\
\Rightarrow & \mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!]) \mathrel{\dot{\mathring{\sqsubseteq}}^{i}} \boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}[\![\mathsf{S}]\!] & \text{(lemma 6)} \\
\Rightarrow & \mathring{\gamma}^{\mathbb{P}^i}(\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!])) \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}[\![\mathsf{S}]\!]) & \text{(def. } \dot{\mathring{\sqsubseteq}}^{i}\text{)} \\
\Rightarrow & \boldsymbol{\mathcal{S}}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!] \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}[\![\mathsf{S}]\!]) & \text{(Galois connection } \langle\wp(\mathbb{S}^{+\infty}_{\mathbb{V}}),\ \subseteq\rangle \xleftrightarrows[\mathring{\alpha}^{\mathbb{P}^i}]{\mathring{\gamma}^{\mathbb{P}^i}} \langle\wp(\mathbb{S}^{+\infty}_{\mathbb{P}^i}),\ \subseteq\rangle,\quad (15)\text{)}
\end{array}
$$

Soundness and calculational design

- Value (real/float) concrete semantics: $\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}]\!]$
- Interval abstract semantics: $\boldsymbol{\mathcal{S}}^*_{\mathbb{P}^i}[\![\mathsf{S}]\!]$
- Soundness: all value (real/float) traces are included in the interval traces:

$$
\begin{array}{lll}
& \mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}]\!]) \mathrel{\mathring{\sqsubseteq}^i} \boldsymbol{\mathcal{S}}^*_{\mathbb{P}^i}[\![\mathsf{S}]\!] & \\
\Rightarrow & \mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}]\!]) \mathrel{\mathring{\sqsubseteq}^i} \boldsymbol{\mathcal{S}}^*_{\mathbb{P}^i}[\![\mathsf{S}]\!] & \wr \text{lemma 6} \int \\
\Rightarrow & \mathring{\gamma}^{\mathbb{P}^i}(\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}]\!])) \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{P}^i}[\![\mathsf{S}]\!]) & \wr \text{def. } \mathring{\sqsubseteq}^i \int \\
\Rightarrow & \boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}]\!] \subseteq \mathring{\gamma}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{P}^i}[\![\mathsf{S}]\!]) & \wr \text{Galois connection } \langle \wp(\mathbb{S}^{+\infty}_{\mathbb{V}}),\ \subseteq\rangle \underset{\mathring{\alpha}^{\mathbb{P}^i}}{\overset{\mathring{\gamma}^{\mathbb{P}^i}}{\leftrightarrows}} \langle \wp(\mathbb{S}^{+\infty}_{\mathbb{P}^i}),\ \subseteq\rangle, \quad (15) \int
\end{array}
$$

- Calculational design:
  - Calculate $\mathring{\alpha}^{\mathbb{P}^i}(\boldsymbol{\mathcal{S}}^*_{\mathbb{V}}[\![\mathsf{S}]\!])$
  - Over approximate by $\mathring{\sqsubseteq}^i$ to eliminate all concrete operations

Calculational design of the float interval trace semantics

Float interval abstraction of an arithmetic expression semantics

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

$$
\begin{array}{rcll}
\mathscr{A}_{\mathbb{P}^i}[\![1]\!]\rho & \triangleq & 1_{\mathbb{P}^i} & \text{where } 1_{\mathbb{P}^i} = [1.0, 1.0] \text{ and } 1.0 \in \mathbb{F} \\
\mathscr{A}_{\mathbb{P}^i}[\![0.1]\!]\rho & \triangleq & 0.1_{\mathbb{P}^i} & \text{where } 0.1_{\mathbb{P}^i} \triangleq [\overleftarrow{]\!]}0.1_{\mathbb{V}}, 0.1_{\mathbb{V}}\overrightarrow{[\![}] \\
\mathscr{A}_{\mathbb{P}^i}[\![x]\!]\rho & \triangleq & \rho(x) & \\
\mathscr{A}_{\mathbb{P}^i}[\![A_1 - A_2]\!]\rho & \triangleq & \mathscr{A}_{\mathbb{P}^i}[\![A_1]\!]\rho \ominus_{\mathbb{P}^i} \mathscr{A}_{\mathbb{P}^i}[\![A_2]\!]\rho & \text{where } [\underline{x}, \overline{x}] \ominus_{\mathbb{P}^i} [\underline{y}, \overline{y}] \triangleq [\underline{x} -_{\mathbb{F}} \overline{y}, \overline{x} -_{\mathbb{F}} \underline{y}]
\end{array}
$$

(with rounding towards $-\infty/\infty$) is such that

$$
\alpha^{\mathbb{P}^i}(\mathscr{A}_{\mathbb{V}}[\![A]\!]\rho) \quad \sqsubseteq^i \quad \mathscr{A}_{\mathbb{P}^i}[\![A]\!]\dot{\alpha}^{\mathbb{P}^i}(\rho). \tag{21}
$$

- $\mathscr{A}_{\mathbb{P}^i}[\![A]\!]$ is $\dot{\sqsubseteq}^i$-increasing (but does not preserves least upper bounds).

Proof

$$
\begin{array}{lll}
- & \alpha^{\mathbb{I}}(\mathscr{A}_{\mathbb{V}}[\![\texttt{0.1}]\!]\rho) & \\
= & \alpha^{\mathbb{I}}(0.1_{\mathbb{V}}) & \text{{ def. } \mathscr{A}_{\mathbb{V}} \text{ in (1)}\}} \\
= & [\lfloor 0.1_{\mathbb{V}}, 0.1_{\mathbb{V}} \rceil] & \text{{ real abstraction by float interval in (14)}\}} \\
\triangleq & \mathscr{A}_{\mathbb{I}}[\![\texttt{0.1}]\!](\alpha^{\mathbb{I}}(\rho)) & \{\text{by defining } \mathscr{A}_{\mathbb{I}}[\![\texttt{0.1}]\!]\overline{\rho} \triangleq [\lfloor 0.1_{\mathbb{V}}, 0.1_{\mathbb{V}} \rceil]\}
\end{array}
$$

$$
\begin{array}{lll}
- & \alpha^{\mathbb{I}}(\mathscr{A}_{\mathbb{V}}[\![\mathsf{x}]\!]\rho) & \\
= & \alpha^{\mathbb{I}}(\rho(\mathsf{x})) & \{\text{def. } \mathscr{A}_{\mathbb{V}} \text{ in (1)}\} \\
= & \alpha^{\mathbb{I}}(\rho)(\mathsf{x}) & \{\text{def. environment abstraction in (14)}\} \\
\triangleq & \mathscr{A}_{\mathbb{I}}[\![\mathsf{x}]\!](\alpha^{\mathbb{I}}(\rho)) & \{\text{by defining } \mathscr{A}_{\mathbb{I}}[\![\mathsf{x}]\!]\overline{\rho} \triangleq \overline{\rho}(\mathsf{x})\}
\end{array}
$$

$$
\begin{array}{lll}
- & \alpha^{\mathbb{I}}(\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1 - \mathsf{A}_2]\!]\rho) & \\
= & \alpha^{\mathbb{I}}(\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho -_{\mathbb{V}} \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho) & \{\text{def. } \mathscr{A}_{\mathbb{V}} \text{ in (1)}\} \\
= & [\lfloor(\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho -_{\mathbb{V}} \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho), (\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho -_{\mathbb{V}} \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho)\rceil] & \{\text{value abstraction by float interval in (14)}\} \\
\sqsubseteq^i & [\lfloor(\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho) -_{\mathbb{F}} (\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho)\rceil, (\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_1]\!]\rho)\rceil -_{\mathbb{F}} \lfloor(\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_2]\!]\rho)] & \{\text{(18) and hyp. (12)}\} \\
\sqsubseteq^i & \text{let } [\underline{x}, \overline{x}] = \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_1]\!]\alpha^{\mathbb{I}}(\rho) \text{ and } [\underline{y}, \overline{y}] = \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_2]\!]\alpha^{\mathbb{I}}(\rho) \text{ in } [\underline{x} -_{\mathbb{F}} \overline{y}, \overline{x} -_{\mathbb{F}} \underline{y}] & \\
 & & \{\text{By ind. hyp. } [\lfloor\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_i]\!]\rho, \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_i]\!]\rho\rceil] = \alpha^{\mathbb{I}}(\mathscr{A}_{\mathbb{V}}[\![\mathsf{A}_i]\!]\rho) \sqsubseteq^i \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_i]\!]\alpha^{\mathbb{I}}(\rho), i = 1, 2.\} \\
= & \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_1]\!]\alpha^{\mathbb{I}}(\rho) -_{\mathbb{I}} \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_2]\!]\alpha^{\mathbb{I}}(\rho) & \{\text{by defining } [\underline{x}, \overline{x}] -_{\mathbb{I}} [\underline{y}, \overline{y}] \triangleq [\underline{x} -_{\mathbb{F}} \overline{y}, \overline{x} -_{\mathbb{F}} \underline{y}]\} \\
\triangleq & \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_1 - \mathsf{A}_2]\!]\alpha^{\mathbb{I}}(\rho) & \{\text{by defining } \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_1 - \mathsf{A}_2]\!]\overline{\rho} \triangleq \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_1]\!]\overline{\rho} -_{\mathbb{I}} \mathscr{A}_{\mathbb{I}}[\![\mathsf{A}_2]\!]\overline{\rho}\}
\end{array}
$$

Approximation:

$$\alpha^{\mathbb{I}}(\{\rho(\mathsf{x}) - \rho(\mathsf{y}) \mid \rho \in \gamma^{\mathbb{I}}(\overline{\rho})\}) \sqsubseteq^i \overline{\rho}(\mathsf{x}) -_{\mathbb{I}} \overline{\rho}(\mathsf{y})$$

Float interval abstraction of an assignment semantics

- $\mathsf{S} ::= {}^{\ell}\ \mathsf{x} = \mathsf{A}\ ;$
- Concrete semantics on reals ($\mathbb{V} = \mathbb{R}$) or float ($\mathbb{V} = \mathbb{F}$):

$$\begin{aligned} \mathcal{S}^{*}_{\mathbb{V}}[\![\mathsf{S}]\!] &= \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \cup \\ &\quad \{\langle \ell,\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho[\mathsf{x} \leftarrow \mathscr{A}_{\mathbb{V}}[\![\mathsf{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{V}}\} \end{aligned} \tag{2}$$

- Abstract semantics on intervals ($\mathbb{V} = \mathbb{P}^{i}$)

$$\begin{aligned} \mathcal{S}^{*}_{\mathbb{P}^{i}}[\![\mathsf{S}]\!] &\triangleq \{\langle \ell,\ \overline{\rho}\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{P}^{i}}\} \cup \\ &\quad \{\langle \ell,\ \overline{\rho}\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \overline{\rho}[\mathsf{x} \leftarrow \mathscr{A}_{\mathbb{P}^{i}}[\![\mathsf{A}]\!]\overline{\rho}]\rangle \mid \overline{\rho} \in \mathbb{E}\mathbb{v}_{\mathbb{P}^{i}}\} \end{aligned}$$

- Same traces except for computing on intervals rather than values

Proof

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

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

Approximation $\dot{\sqsubseteq}^{i}$:

- value $\mathscr{A}_{\mathbb{V}}$ to interval arithmetic $\mathscr{A}_{\mathbb{I}}$
- value to interval environments

Float interval abstraction of an arithmetic expression semantics

- A test is true or false for $\mathbb{V} = \mathbb{R}$ and $\mathbb{V} = \mathbb{F}$
- For intervals a test is imprecise (e.g. $<$ is handled as $\leqslant$), may yield a split, and overlap.
- The abstract interpretation $\mathscr{B}_{\mathbb{P}^i}[\![\mathsf{B}]\!]$ of a boolean expression B is defined such that

$$
\begin{array}{l}
\text{let } \langle\overline{\rho}_{\mathsf{tt}},\ \overline{\rho}_{\mathsf{ff}}\rangle = \mathscr{B}_{\mathbb{P}^i}[\![\mathsf{B}]\!]\dot{\alpha}^{\mathbb{P}^i}(\rho) \text{ in} \\
\qquad \begin{array}{lllll}
\dot{\alpha}^{\mathbb{P}^i}(\rho) & \dot{\sqsubseteq}^i & \overline{\rho}_{\mathsf{tt}} & \text{if} & \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \\
\dot{\alpha}^{\mathbb{P}^i}(\rho) & \dot{\sqsubseteq}^i & \overline{\rho}_{\mathsf{ff}} & \text{if} & \mathscr{B}_{\mathbb{V}}[\![\mathsf{B}]\!]\rho = \mathsf{ff}
\end{array} \\
\text{and } (\langle\overline{\rho}_{\mathsf{tt}},\ \overline{\rho}_{\mathsf{ff}}\rangle = \mathscr{B}_{\mathbb{P}^i}[\![\mathsf{B}]\!]\overline{\rho}) \Rightarrow (\overline{\rho}_{\mathsf{tt}}\ \dot{\sqsubseteq}^i\ \overline{\rho} \wedge \overline{\rho}_{\mathsf{ff}}\ \dot{\sqsubseteq}^i\ \overline{\rho})
\end{array}
\tag{22}
$$

- No concrete state passing the test is omitted in the abstract, and
- The postcondition $\overline{\rho}_{\mathsf{tt}}$ or $\overline{\rho}_{\mathsf{ff}}$ is stronger than the precondition $\overline{\rho}$ (no side effects)

Float interval abstraction of a conditional

- Conditional statement $\mathsf{S} ::= \mathtt{if}\ \ell\ (\mathsf{B})\ \mathsf{S}_t$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)[3]

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

- Most libraries raise an error exception in case of split (or chose only one branch).

$$
\begin{aligned}
\boldsymbol{\mathcal{S}}^{*}_{\mathbb{P}^i}[\![\mathsf{S}]\!] \quad \triangleq \quad & \cdots \\
& \cup \{\langle \ell,\ \overline{\rho}\rangle\pi \mid \exists \overline{\rho}_{\mathrm{tt}}, \overline{\rho}_{\mathrm{ff}}\ .\ \mathcal{B}_{\mathbb{P}^i}[\![\mathsf{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathrm{tt}},\ \overline{\rho}_{\mathrm{ff}}\rangle \wedge \rho_{\mathrm{tt}}\ \dot{\sqcap}^i\ \rho_{\mathrm{ff}} \neq \dot{\varnothing} \wedge \pi \in \mathbb{S}^{+\infty}_{\mathbb{P}^i}\}
\end{aligned}
$$

---

[3] We assume that $\dot{\gamma}^{\mathbb{I}}(\dot{\varnothing}) = \varnothing$.

Float interval abstraction of an iteration

- Iteration statement $\mathsf{S} ::= \mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$\mathcal{S}^*_{\mathbb{P}^i}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] = \mathsf{lfp}^{\subseteq}\, \mathcal{F}^*_{\mathbb{P}^i}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] \tag{8bis}$$

$$\begin{aligned}
\mathcal{F}^*_{\mathbb{P}^i}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]\, X \triangleq\ & \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}_{\mathbb{P}^i}\} \\
& \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho_{\mathsf{ff}}\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge{} \\
& \qquad \exists \overline{\rho}_{\mathsf{tt}}\ .\ \mathcal{B}_{\mathbb{P}^i}[\![\mathsf{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathsf{tt}},\ \overline{\rho}_{\mathsf{ff}}\rangle \wedge \rho_{\mathsf{ff}} \neq \dot{\varnothing} \wedge \ell' = \ell\} \\
& \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho_{\mathsf{tt}}\rangle\pi_3 \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge{} \\
& \qquad \exists \overline{\rho}_{\mathsf{ff}}\ .\ \mathcal{B}_{\mathbb{P}^i}[\![\mathsf{B}]\!]\overline{\rho} = \langle \overline{\rho}_{\mathsf{tt}},\ \overline{\rho}_{\mathsf{ff}}\rangle \wedge \rho_{\mathsf{tt}} \neq \dot{\varnothing} \wedge{} \\
& \qquad\quad \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho_{\mathsf{tt}}\rangle\pi_3 \in \mathcal{S}^*_{\mathbb{P}^i}[\![\mathsf{S}_b]\!] \wedge \ell' = \ell\}
\end{aligned}$$

Abstraction to a transition system

Abstraction to a transition system

- Abstraction to a transition system

$$\begin{array}{rcl}\alpha_t(\pi) & \triangleq & \{\langle\sigma_1,\ \sigma_2\rangle \mid \exists\pi_1,\pi_2\ .\ \pi = \pi_1\sigma_1\sigma_2\pi_2\}\\ \alpha_T(\Pi) & \triangleq & \bigcup_{\pi\in\Pi}\alpha_t(\pi)\end{array}$$

- Provides a small-step operational semantics of the program (specifying an implementation)
- We used trace abstractions so there is no need for [bi-]simulations, etc. in the proof of correctness of the implementation

Improving precision

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.

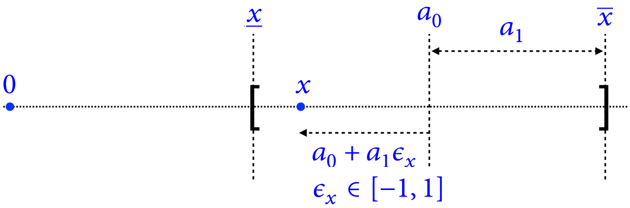
Affine arithmetic

- 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

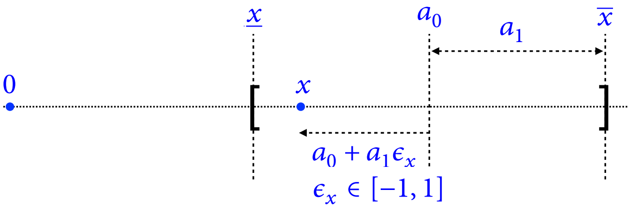
  $x = a_0 + a_1\epsilon_x$ where $a_0 = \frac{\overline{x}+\underline{x}}{2}$, $a_1 = \frac{\overline{x}-\underline{x}}{2}$, and $\epsilon_x \in [-1, 1]$ is a fresh auxiliary variable.



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.



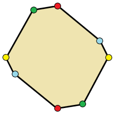
- Then $x - x = (a_0 + a_1\epsilon_x) - (a_0 + a_1\epsilon_x) = 0 + 0\epsilon_x$, as required.

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 $[-1, +1]$.

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

Conclusion

- Interval arithmetics in scientific computing put bounds on rounding errors in floating point arithmetic [Moore, 1966].
- It is an abstract interpretation of the trace semantics and can be computed at runtime for one trace at a time.
- Tests may have to consider many executions, which can be quite inefficient (and often considered an error in practice).
- A further abstract yields the static interval analysis (by joining states on paths at each program point to get invariants).
- More generally, this provides a framework for dynamic analysis (their static over approximation, and the combination of the two).
- Soundness guarantee!

Bibliography

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.". *IEEE SIBGRAPI.*, pp. 9–18.

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

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

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

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.

Bibliography II

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

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.

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

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

The End, Thank you

The slides are available at:

http://cs.nyu.edu/ pcousot/publications.www/slidesPCousot-SOAP-2021.pdf