Principles of Abstract Interpretation
MIT press
Ch. **28**, Abstract cartesian semantics

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-28--cartesian-reachability-semantics-PrAbsInt.pdf

Chapter 28

Ch. **28**, Abstract cartesian semantics

Definition of a Static Analyzer

- Given an abstract domain $\mathbb{D}^\natural$, a static analyzer must, for any program $\mathtt{P}$ of a language $\mathscr{P}$, find an abstract inductive invariant $\mathcal{I} \in \mathsf{labs}[\![\mathtt{P}]\!] \to \mathbb{D}^\natural$ satisfying the verification conditions $\mathscr{V}^\natural[\![\mathtt{P}]\!]\mathcal{I}$ of Chapter **25** (Abstract reachability/invariance/safety verification semantics) and strong enough to imply a correctness specification $\mathcal{S}^\natural[\![\mathtt{P}]\!] \in \mathsf{labs}[\![\mathtt{P}]\!] \to \mathbb{D}^\natural$.

- The most difficult part is "find an abstract inductive invariant $\mathcal{I} \in \mathsf{labs}[\![\mathtt{P}]\!] \to \mathbb{D}^\natural$" (*i.e.* find the inductive argument in an inductive proof)

- One way to solve this difficulty is to be "more abstract"

- This is the case of cartesian abstractions which are more abstract than relational abstractions (expressing relations between values of variables)

Introduction to Cartesian abstraction and Examples

Cartesian abstraction

The cartesian abstraction abstracts

a relational property expressing a relation between values of variables

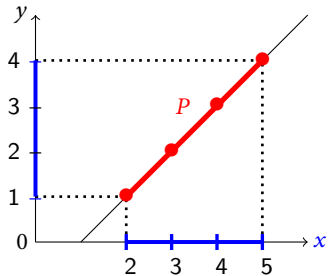
into

a conjunction of unrelated properties on the values of each variables

(which are independent of the values of the other variables)

Cartesian abstraction (contn'd)

- Cartesian abstraction of property $P \triangleq (x = y + 1 \wedge y \in [1, 4])$ is $\dot{\alpha}_{\vec{x}}(P) \triangleq (x \in [2, 5] \wedge y \in [1, 4])$ so that the relation $x = y + 1$ is lost.
- This is René Descartes' projection on the axes of a coordinate system [Descartes, 1637].



Cartesian abstraction (contn'd)

- Because relational information is lost, the cartesian abstraction is mainly applied to assertional invariants (rather than relational invariants since the relation to initial values of variables is lost by the abstraction).
- Formally,

$$\begin{array}{rcl} \mathbb{E}\mathbb{v} & = & \mathbb{V} \to \mathbb{V} \\ \dot{\alpha}_{\mathbb{x}}(P) & \triangleq & \mathtt{x} \in \mathbb{V} \mapsto \{\rho(\mathtt{x}) \mid \rho \in P\} \\ \dot{\gamma}_{\mathbb{x}}(\overline{P}) & \triangleq & \{\rho \in \mathbb{E}\mathbb{v} \mid \forall \mathtt{x} \in \mathbb{V} \,.\, \rho(\mathtt{x}) \in \overline{P}(\mathtt{x})\} \end{array} \tag{28.1}$$

$$\langle \wp(\mathbb{V} \to \mathbb{V}), \subseteq \rangle \underset{\dot{\alpha}_{\mathbb{x}}}{\overset{\dot{\gamma}_{\mathbb{x}}}{\leftrightarrows}} \langle \mathbb{V} \to \wp(\mathbb{V}), \dot{\subseteq} \rangle$$

Cartesian abstraction (contn'd)

- Pointwise extension to variable properties attached program points $\ddot{\alpha}_{\vec{x}}(P)^\ell \triangleq \dot{\alpha}_{\vec{x}}(P(\ell))$

$$\langle \mathbb{L} \to \wp(\mathbb{V} \to \mathbb{V}),\ \dot{\subseteq} \rangle \underset{\ddot{\alpha}_{\vec{x}}}{\overset{\ddot{\gamma}_{\vec{x}}}{\leftrightarrows}} \langle \mathbb{L} \to (\mathbb{V} \to \wp(\mathbb{V})),\ \ddot{\subseteq} \rangle$$

- Extension to cartesian transformers of initial cartesian properties of variables to cartesian variable properties attached to program points $\vec{\alpha}_{\vec{x}}(T)\overline{\rho} \triangleq \ddot{\alpha}_{\vec{x}}(T(\dot{\gamma}_{\vec{x}}(\overline{\rho})))$.

$$\langle \wp(\mathbb{V} \to \mathbb{V}) \to (\mathbb{L} \to \wp(\mathbb{V} \to \mathbb{V})),\ \ddot{\subseteq} \rangle \underset{\vec{\alpha}_{\vec{x}}}{\overset{\vec{\gamma}_{\vec{x}}}{\leftrightarrows}} \langle (\mathbb{V} \to \wp(\mathbb{V})) \to (\mathbb{L} \to (\mathbb{V} \to \wp(\mathbb{V}))),\ \ddot{\subseteq} \rangle$$

Cartesian reachability semantics

- The cartesian reachability semantics is then

$$\vec{\alpha}_{\vec{\times}}(\boldsymbol{\mathcal{S}}^{\vec{r}}[\![\mathtt{P}]\!]) \quad \ddot{\subseteq} \quad \boldsymbol{\mathcal{S}}^{\vec{\times}}[\![\mathtt{P}]\!] \tag{28.5}$$

(or equality for an exact abstraction in case of completeness).

Loss of precision of the structural cartesian reachability semantics of programs

- The definition (28.5) of the cartesian reachability semantics involves the calculation of the reachability semantics in the concrete domain
$$\wp(\mathbb{E}\mathbb{v}) \to (\mathbb{L} \to \wp(\mathbb{E}\mathbb{v}))$$
- And then its abstraction into the abstract domain
$$(\mathbb{V} \to \wp(\mathbb{V})) \to (\mathbb{L} \to (\mathbb{V} \to \wp(\mathbb{V})))$$
by the cartesian abstraction $\vec{\alpha}_{\times}$.
- We look for a structural cartesian reachability semantics $\widehat{\mathcal{S}}^{\times}[\![\mathtt{P}]\!]$ calculated by structural induction on the program in the abstract domain only.
- This necessarily involves a loss of precision.

Abstract cartesian semantics

- Since the set $\mathbb{V}$ of values is usually very large, if not infinite, the cartesian reachability domain $(\mathcal{V} \to \wp(\mathbb{V})) \to (\mathcal{L} \to (\mathcal{V} \to \wp(\mathbb{V})))$ is hardly machine representable.
- It is therefore necessary to introduce a further value property abstraction

$$\langle \wp(\mathbb{V}), \subseteq \rangle \underset{\alpha_\times}{\overset{\gamma_\times}{\leftrightarrows}} \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$$

- Pointwise extension to cartesian environment properties $\dot{\alpha}_\times(\overline{\rho})\mathtt{x} \triangleq \alpha_\times(\overline{\rho}(\mathtt{x}))$

$$\langle \mathcal{V} \to \wp(\mathbb{V}), \dot{\subseteq} \rangle \underset{\dot{\alpha}_\times}{\overset{\dot{\gamma}_\times}{\leftrightarrows}} \langle \mathcal{V} \to \mathbb{P}^\times, \dot{\sqsubseteq}^\times \rangle$$

- Pointwise extension again to local cartesian properties attached to program points $\ddot{\alpha}_\times(\dot{P})\ell \triangleq \dot{\alpha}_\times(\dot{P}(\ell))$

$$\langle \mathcal{L} \to (\mathcal{V} \to \wp(\mathbb{V})), \ddot{\subseteq} \rangle \underset{\ddot{\alpha}_\times}{\overset{\ddot{\gamma}_\times}{\leftrightarrows}} \langle \mathcal{L} \to (\mathcal{V} \to \mathbb{P}^\times), \ddot{\sqsubseteq}^\times \rangle$$

Abstract cartesian semantics (Cont'd)

- Functional extension to transformers of cartesian initial conditions
  $\vec{\alpha}_\times(\overline{T}) \triangleq \ddot{\alpha}_\times \circ \overline{T} \circ \dot{\gamma}_\times$

$$\langle (\mathscr{V} \to \wp(\mathbb{V})) \to (\mathscr{L} \to (\mathscr{V} \to \wp(\mathbb{V}))), \ddot{\subseteq} \rangle \underset{\vec{\alpha}_\times}{\overset{\vec{\gamma}_\times}{\leftrightarrows}} \langle (\mathscr{V} \to \mathbb{P}^\times) \to (\mathscr{L} \to (\mathscr{V} \to \mathbb{P}^\times)), \ddot{\sqsubseteq}^\times \rangle$$

- By composition, we have

$$\langle \wp(\mathscr{V} \to \mathbb{V}) \to (\mathscr{L} \to \wp(\mathscr{V} \to \mathbb{V})), \ddot{\subseteq} \rangle \underset{\vec{\alpha}_\times \circ \vec{\alpha}_{\vec{\times}}}{\overset{\vec{\gamma}_{\vec{\times}} \circ \vec{\gamma}_\times}{\leftrightarrows}} \langle (\mathscr{V} \to \mathbb{P}^\times) \to (\mathscr{L} \to (\mathscr{V} \to \mathbb{P}^\times)), \ddot{\sqsubseteq}^\times \rangle$$

- The abstract cartesian reachability semantics $\mathscr{S}^\times[\![\mathsf{P}]\!]$ must then be such that

$$\vec{\alpha}_\times(\mathscr{S}^{\vec{\times}}[\![\mathsf{P}]\!]) \quad = \quad \vec{\alpha}_\times(\vec{\alpha}_{\vec{\times}}(\mathscr{S}^{\vec{r}}[\![\mathsf{P}]\!])) \quad \ddot{\sqsubseteq}^\times \quad \mathscr{S}^\times[\![\mathsf{P}]\!] \tag{28.6}$$

  (or equality for an exact abstraction in case of completeness).

Abstract cartesian semantics (Cont'd)

- In absence of best abstraction, use increasing concretizations only, with

$$\boldsymbol{\mathcal{S}}^{\vec{r}}[\![\mathsf{P}]\!] \mathrel{\ddot{\subseteq}} \vec{\gamma}_{\vec{x}} \circ \vec{\gamma}_{\times}(\boldsymbol{\mathcal{S}}^{\times}[\![\mathsf{P}]\!])$$

- The abstraction $\dot{\alpha}_{\times}$ of $\langle \mathscr{V} \to \wp(\mathbb{V})), \dot{\subseteq} \rangle$ into $\langle \mathscr{V} \to \mathbb{P}^{\times}, \dot{\sqsubseteq}^{\times} \rangle$ will in general use a different abstract domain $\mathbb{P}^{\times}$ for different variables.

- Moreover, the cartesian abstraction may not be pointwise for each variable[1], but into an abstract domain $\langle \mathbb{P}^{\natural}, \dot{\sqsubseteq}^{\natural} \rangle$.

[1] For example, one might be interested in the union of the sets of possible values of a group of variables.

Characterization of cartesian abstractions

- By Exercises 28.2 and 11.55, $\dot{\gamma}_\times \circ \dot{\alpha}_\times$ is an upper closure operator.
- This can be used to define cartesian abstractions as those for which $\dot{\gamma}_\times \circ \dot{\alpha}_\times$ causes no additional loss of information.

Definition 28.7 (Cartesian abstraction) An abstraction $\gamma \in \mathbb{D}^\sharp \xrightarrow{\curvearrowright} \wp(\mathbb{V} \mapsto \mathbb{V})$ is *cartesian* if and only if $\gamma = \dot{\gamma}_\times \circ \dot{\alpha}_\times \circ \gamma$.

Structural cartesian reachability semantics of programs

Example

reachability semantics $\mathcal{S}^{\vec{r}}[\![\mathsf{P}]\!](\dot{\gamma}_x(\overline{\rho}))\ell$	cartesian abstraction $\mathcal{S}^{\times}[\![\mathsf{P}]\!](\overline{\rho})\ell \triangleq \dot{\alpha}_{\vec{x}}(\mathcal{S}^{\vec{r}}[\![\mathsf{P}]\!](\dot{\gamma}_x(\overline{\rho}))\ell)$
ℓ_1 /* $\dot{\gamma}_x(\overline{\rho}) = 0 \leqslant x \leqslant 2$ */	ℓ'_1 /* $\dot{\gamma}_x(\overline{\rho}) = 0 \leqslant x \leqslant 2$ */
y = x ;	y = x ;
ℓ_2 /* $0 \leqslant x = y \leqslant 2$ */	ℓ'_2 /* $0 \leqslant x \leqslant 2 \wedge 0 \leqslant y \leqslant 2$ */
z = y − x ;	z = y − x ;
ℓ_3 /* $0 \leqslant x = y \leqslant 2 \wedge z = 0$ */	ℓ'_3 /* $0 \leqslant x \leqslant 2 \wedge 0 \leqslant y \leqslant 2 \wedge z = 0$ */

- The structural cartesian reachability semantics will derive that $0 \leqslant x \leqslant 2 \wedge 0 \leqslant y \leqslant 2$ holds after the assignment y = x ;.
- But then it is unknown that $x - y$ so, without this information, it is impossible to know that $z = 0$ after the assignment z = y − x ;.

Example (cont'd)

- So the structural cartesian reachability semantics will be

$$\widehat{\mathcal{S}}^{\times}[\![\mathsf{P}]\!](\overline{\rho})\ell$$

ℓ_1 /* $\dot{\gamma}_{\times}(\overline{\rho}) = 0 \leqslant x \leqslant 2$ */

y = x ;

ℓ_2 /* $0 \leqslant x \leqslant 2 \wedge 0 \leqslant y \leqslant 2$ */

z = y − x ;

ℓ_3 /* $0 \leqslant x \leqslant 2 \wedge 0 \leqslant y \leqslant 2 \wedge -2 \leqslant z \leqslant 2$ */

□

Inductive hierarchy of abstract cartesian semantics

Program properties abstractions

$\ddot{\mathbb{D}}^{\natural} \triangleq \langle (\mathscr{V} \to \mathbb{P}^{\natural}) \to (\mathscr{L} \to (\mathscr{V} \to \mathbb{P}^{\natural})),\ \ddot{\sqsubseteq}^{\natural},\ \ddot{\mathrm{I}}^{\natural},\ \ddot{\cup}^{\natural},\ \mathrm{assign}^{\natural}[\![\mathtt{x},\mathtt{A}]\!],\ \mathrm{test}^{\natural}[\![\mathtt{B}]\!],\ \overline{\mathrm{test}}^{\natural}[\![\mathtt{B}]\!] \rangle$ $\quad \widehat{\mathcal{S}}^{\natural}[\![\mathtt{P}]\!]$ abstract cartesian semantics (28.9)

$\vec{\alpha}_{\natural} \uparrow\downarrow \vec{\gamma}_{\natural}$ $\quad \downarrow \vec{\gamma}_{\natural}$

$\times$

$\vdots\sqcup\!\mid$

$\ddot{\mathbb{D}}^{\times} \triangleq \langle (\mathscr{V} \to \mathbb{P}^{\times}) \to (\mathscr{L} \to (\mathscr{V} \to \mathbb{P}^{\times})),\ \ddot{\sqsubseteq}^{\times},\ \ddot{\mathrm{I}}^{\times},\ \ddot{\cup}^{\times},\ \mathrm{assign}^{\times}[\![\mathtt{x},\mathtt{A}]\!],\ \mathrm{test}^{\times}[\![\mathtt{B}]\!],\ \overline{\mathrm{test}}^{\times}[\![\mathtt{B}]\!] \rangle$ $\quad \widehat{\mathcal{S}}^{\times}[\![\mathtt{P}]\!]$ cartesian semantics

$\vec{\alpha}_{\times} \uparrow\downarrow \vec{\gamma}_{\times}$ $\quad \downarrow \vec{\gamma}_{\times}$

$\cdots$ $\quad \cdots$

$\uparrow\downarrow$ $\quad \downarrow$

$\vdots\sqcup\!\mid$

$\dddot{\mathbb{D}}^{\vec{\times}} \triangleq \langle (\mathscr{V} \to \wp(\mathbb{V})) \to (\mathscr{L} \to (\mathscr{V} \to \wp(\mathbb{V}))),\ \ddot{\subseteq},\ \ddot{\varnothing},\ \ddot{\cup},\ \mathrm{assign}^{\vec{\times}}[\![\mathtt{x},\mathtt{A}]\!],\ \mathrm{test}^{\vec{\times}}[\![\mathtt{B}]\!],\ \overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{B}]\!] \rangle$ $\quad \widehat{\mathcal{S}}^{\vec{\times}}[\![\mathtt{P}]\!]$ cartesian reachability semantics

$\vec{\alpha}_{\vec{\times}} \uparrow\downarrow \vec{\gamma}_{\vec{\times}}$ $\quad \downarrow \vec{\gamma}_{\vec{\times}}$

$\vdots\sqcup\!\mid$

$\ddot{\mathbb{D}}^{\vec{r}} \triangleq \langle \wp(\mathbb{E}\mathtt{v}) \to (\mathscr{L} \to \wp(\mathbb{E}\mathtt{v})),\ \ddot{\subseteq}, \ddot{\varnothing}\ \ddot{\cup},\ \mathrm{assign}^{\vec{r}}[\![\mathtt{x},\mathtt{A}]\!],\ \mathrm{test}^{\vec{r}}[\![\mathtt{B}]\!],\ \overline{\mathrm{test}}^{\vec{r}}[\![\mathtt{B}]\!] \rangle$ $\quad \widehat{\mathcal{S}}^{\vec{r}}[\![\mathtt{P}]\!]$ assertional reachability semantics

Value properties abstractions

The abstract cartesian domain for program properties can be parameterized by a value abstract domain (as shown by the calculational design).

$$\mathbb{D}^{\natural} \triangleq \langle \mathbb{P}^{\natural}, \sqsubseteq^{\natural}, \bot^{\natural}, \top^{\natural}, \sqcup^{\natural}, \sqcap^{\natural}, 1^{\natural}, \ominus^{\natural}, \ominus^{\natural_1}, \circledcirc^{\natural}, \overline{\circledcirc}^{\natural} \rangle \quad \text{abstract cartesian value domain} \qquad (28.10)$$

$$\alpha_{\natural} \uparrow\downarrow \gamma_{\natural}$$

$$\mathbb{D}^{\times} \triangleq \langle \mathbb{P}^{\times}, \sqsubseteq^{\times}, \bot^{\times}, \top^{\times}, \sqcup^{\times}, \sqcap^{\times}, 1^{\times}, \ominus^{\times}, \ominus^{\times_1}, \circledcirc^{\times}, \overline{\circledcirc}^{\times} \rangle \quad \text{cartesian value domain}$$

$$\alpha_{\times} \uparrow\downarrow \gamma_{\times}$$

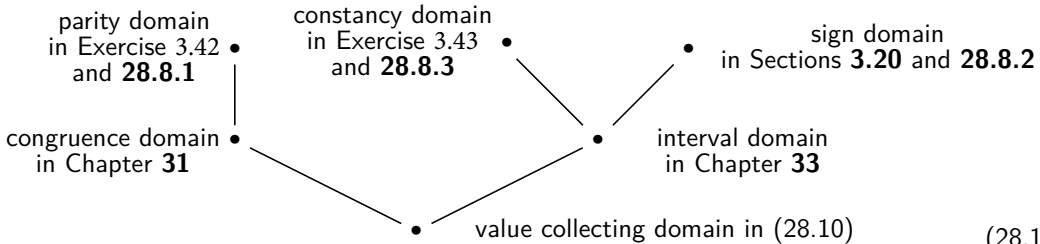
$$\dots$$

$$\uparrow\downarrow$$

$$\mathbb{D}^{\vec{\times}} \triangleq \langle \wp(\mathbb{V}), \subseteq, \varnothing, \mathbb{V}, \cup, \cap, \{1\}, \ominus^{\vec{\times}}, \ominus^{\vec{\times}_1}, \circledcirc^{\vec{\times}}, \overline{\circledcirc}^{\vec{\times}} \rangle \quad \text{value collecting domain}$$

Hierarchy of cartesian abstractions

Here is a small subset:



(28.11)

Cartesian static analysis of arithmetic expressions (I/II)

To do

- To get an abstract cartesian semantics, we proceed in 3 steps:
  1. Abstract from the reachability semantics
     $\mathcal{S}^{\vec{r}}[\![\mathtt{P}]\!] \circ \dot{\gamma}_{\times} \in (\mathcal{V} \to \wp(\mathbb{V})) \mathrel{-\!\!\!\rightarrow\!\!\!\!\nearrow} (\mathcal{L} \to \wp(\mathbb{E}\mathtt{v}))$
     into the cartesian semantics
     $\widehat{\mathcal{S}}^{\times}[\![\mathtt{P}]\!] \in (\mathcal{V} \to \wp(\mathbb{V})) \mathrel{-\!\!\!\rightarrow\!\!\!\!\nearrow} (\mathcal{L} \to (\mathcal{V} \to \wp(\mathbb{V})))$
  2. Further abstract sets of values (that may be too large or infinite) by
     $\gamma_{\natural} \in \langle \mathbb{P}^{\natural}, \sqsubseteq^{\natural} \rangle \mathrel{-\!\!\!\rightarrow\!\!\!\!\nearrow} \langle \wp(\mathbb{V}), \subseteq \rangle$
  3. Extend pointwise to cartesian abstract semantics
     $\widehat{\mathcal{S}}^{\natural}[\![\mathtt{P}]\!] \in (\mathcal{V} \to \mathbb{P}^{\natural}) \mathrel{-\!\!\!\rightarrow\!\!\!\!\nearrow} (\mathcal{L} \to (\mathcal{V} \to \mathbb{P}^{\natural}))$
- We just have to do this for arithmetic/boolean expressions (since then the abstract interpreter soundness follows by Theorem 27.4)

To do

(1) Abstract the reachability/forward/post semantics of arithmetic expressions into a cartesian reachability/forward semantics of
   (1.a) arithmetic expressions
   (1.b) assignment statements

(2) Abstract the cartesian reachability/forward semantics into an abstract cartesian reachability/forward semantics of
   (2.a) arithmetic expressions
   (2.b) assignment statements

(3) Idem for the accessibility/backward/pre semantics
   (3.a) accessibility semantics
   (3.b) cartesian accessibility semantics
   (3.c) abstract cartesian accessibility semantics

   for arithmetic expressions and assignment statements

Calculational design of the cartesian reachability semantics of arithmetic expressions

Let us make a *first attempt* to define the cartesian evaluation of arithmetic expressions for $\overline{\rho} \in \mathbb{V} \to \mathbb{P}^{\vec{\mathbb{X}}}$, $\mathbb{P}^{\vec{\mathbb{X}}} = \wp(\mathbb{V})$,

Tentative cartesian reachability semantics of an arithmetic expression A

$$
\begin{array}{rcl}
\mathscr{A}^{\vec{\mathbb{X}}}[\![1]\!]\,\overline{\rho} & \triangleq & 1^{\vec{\mathbb{X}}} \quad \text{where} \quad 1^{\vec{\mathbb{X}}} = \{1\} \\
\mathscr{A}^{\vec{\mathbb{X}}}[\![x]\!]\,\overline{\rho} & \triangleq & \overline{\rho}(x) \\
\mathscr{A}^{\vec{\mathbb{X}}}[\![A_1 - A_2]\!]\,\overline{\rho} & \triangleq & \mathscr{A}^{\vec{\mathbb{X}}}[\![A_1]\!]\,\overline{\rho} \ominus^{\vec{\mathbb{X}}} \mathscr{A}^{\vec{\mathbb{X}}}[\![A_2]\!]\,\overline{\rho} \\
X \ominus^{\vec{\mathbb{X}}} Y & \triangleq & \{x - y \mid x \in X \wedge y \in Y\}
\end{array}
$$

Let us define the cartesian evaluation of arithmetic expressions for $\overline{\rho} \in \mathbb{V} \to \mathbb{P}^{\vec{\mathbb{X}}}$, $\mathbb{P}^{\vec{\mathbb{X}}} = \wp(\mathbb{V})$,

Cartesian reachability semantics of an arithmetic expression A

$$
\begin{array}{rcll}
\mathbb{O}^{\vec{\mathbb{X}}}(\overline{P})\,\overline{\rho} & \triangleq & \llbracket\, \overline{\rho} = \dot{\varnothing} \;?\; \varnothing \;:\; \overline{P} \,\rrbracket & \text{smash} \\
\mathscr{A}^{\vec{\mathbb{X}}}[\![1]\!]\,\overline{\rho} & \triangleq & \mathbb{O}^{\vec{\mathbb{X}}}(1^{\vec{\mathbb{X}}})\,\overline{\rho} \quad \text{where} \quad 1^{\vec{\mathbb{X}}} = \{1\} & (28.13) \\
\mathscr{A}^{\vec{\mathbb{X}}}[\![\mathtt{x}]\!]\,\overline{\rho} & \triangleq & \mathbb{O}^{\vec{\mathbb{X}}}(\overline{\rho}(\mathtt{x}))\,\overline{\rho} & \\
\mathscr{A}^{\vec{\mathbb{X}}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\,\overline{\rho} & \triangleq & \mathbb{O}^{\vec{\mathbb{X}}}(\mathscr{A}^{\vec{\mathbb{X}}}[\![\mathtt{A}_1]\!]\,\overline{\rho} \ominus^{\vec{\mathbb{X}}} \mathscr{A}^{\vec{\mathbb{X}}}[\![\mathtt{A}_2]\!]\,\overline{\rho})\,\overline{\rho} & \\
X \ominus^{\vec{\mathbb{X}}} Y & \triangleq & \{x - y \mid x \in X \wedge y \in Y\} &
\end{array}
$$

so that

Lemma (28.14) $\mathscr{A}^{\vec{\mathbb{r}}}[\![\mathtt{A}]\!] \mathrel{\dot{\subseteq}} \mathscr{A}^{\vec{\mathbb{X}}}[\![\mathtt{A}]\!] \circ \dot{\alpha}_{\vec{\mathbb{x}}}$.

Proof of Lemma 28.14 The inclusion is trivial when $\overline{\rho} = \varnothing$ (which is equivalent to $\dot{\alpha}_{\vec{x}}(\overline{\rho}) = \dot{\varnothing}$). Otherwise, by structural induction on arithmetic expressions, for all $\overline{\rho} \in \wp(\mathbb{V} \to \mathbb{V})$.

— $\mathscr{A}^{\vec{r}}[\![1]\!]\,\overline{\rho}$

$= \{\mathscr{A}[\![1]\!]\,\rho \mid \rho \in \overline{\rho}\}$ ⟅(28.12)⟆

$= \{1\}$ ⟅def. (3.4) of $\mathscr{A}$ and $\overline{\rho} \neq \varnothing$⟆

$= \mathscr{A}^{\vec{x}}[\![1]\!]\dot{\alpha}_{\vec{x}}(\overline{\rho})$ ⟅since $\overline{\rho} \neq \varnothing$ so $\dot{\alpha}_{\vec{x}}(\overline{\rho}) \neq \dot{\varnothing}$ and (28.13)⟆

— $\mathscr{A}^{\vec{r}}[\![x]\!]\,\overline{\rho}$

$= \{\mathscr{A}[\![x]\!]\,\rho \mid \rho \in \overline{\rho}\}$ ⟅(28.12)⟆

$= \{\rho(x) \mid \rho \in \overline{\rho}\}$ ⟅def. (3.4) of $\mathscr{A}$ and $\overline{\rho} \neq \varnothing$⟆

$= \dot{\alpha}_{\vec{x}}(\overline{\rho})x$ ⟅def. (28.1) of $\dot{\alpha}_{\vec{x}}$⟆

$= \mathscr{A}^{\vec{x}}[\![x]\!]\dot{\alpha}_{\vec{x}}(\overline{\rho})$ ⟅since $\overline{\rho} \neq \varnothing$ so $\dot{\alpha}_{\vec{x}}(\overline{\rho}) \neq \dot{\varnothing}$ and (28.13)⟆

$$
\begin{array}{lll}
= & \mathscr{A}^{\vec{r}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\,\overline{\rho} & \\
= & \{\mathscr{A}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\,\rho \mid \rho \in \overline{\rho}\} & \text{(28.12)} \\
= & \{\mathscr{A}[\![\mathtt{A}_1]\!]\,\rho - \mathscr{A}[\![\mathtt{A}_2]\!]\,\rho \mid \rho \in \overline{\rho}\} & \text{def. (3.4) of } \mathscr{A} \\
\subseteq & \{x - y \mid x \in \{\mathscr{A}[\![\mathtt{A}_1]\!]\,\rho \mid \rho \in \overline{\rho}\} \wedge y \in \{\mathscr{A}[\![\mathtt{A}_2]\!]\,\rho \mid \rho \in \overline{\rho}\}\} & \\
 & & \text{loosing relationships between variables} \\
\subseteq & \{x - y \mid x \in \mathscr{A}^{\vec{\mathtt{x}}}[\![\mathtt{A}_1]\!]\dot{\alpha}_{\vec{\mathtt{x}}}(\overline{\rho}) \wedge y \in \mathscr{A}^{\vec{\mathtt{x}}}[\![\mathtt{A}_2]\!]\dot{\alpha}_{\vec{\mathtt{x}}}(\overline{\rho})\} & \text{structural induction hypothesis and } \overline{\rho} \neq \varnothing \\
= & \mathscr{A}^{\vec{\mathtt{x}}}[\![\mathtt{A}_1]\!]\dot{\alpha}_{\vec{\mathtt{x}}}(\overline{\rho}) \ominus^{\vec{\mathtt{x}}} \mathscr{A}^{\vec{\mathtt{x}}}[\![\mathtt{A}_2]\!]\dot{\alpha}_{\vec{\mathtt{x}}}(\overline{\rho}) & \text{by def. } \ominus^{\vec{\mathtt{x}}} \text{ in (28.13)} \\
= & \mathscr{A}^{\vec{\mathtt{x}}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\dot{\alpha}_{\vec{\mathtt{x}}}(\overline{\rho}) & \text{since } \overline{\rho} \neq \varnothing \text{ so } \dot{\alpha}_{\vec{\mathtt{x}}}(\overline{\rho}) \neq \dot{\varnothing} \text{ and def. (28.13) of } \mathscr{A}^{\vec{\mathtt{x}}}[\![\mathtt{A}_1 - \mathtt{A}_2]\!] \quad \square
\end{array}
$$

Structural cartesian reachability/forward semantics of assignment

- It remains to calculate the abstract transformer $\mathsf{assign}^{\vec{\mathsf{x}}}[\![\mathsf{x}, \mathsf{A}]\!]$ (and more generally $f^{\vec{\mathsf{x}}}$) satisfying Definition 27.1-I-2 and, based on Corollary 27.20, the best abstraction of $\mathsf{assign}^{\vec{\mathsf{r}}}[\![\mathsf{x}, \mathsf{A}]\!]$ (and more generally $f^{\vec{\mathsf{r}}}$).

- Since we have a Galois connection, there are essentially two alternatives.
  (1) Expand the definitions of $\dot{\alpha}_{\vec{x}}$, $\dot{\gamma}_{\vec{x}}$, and the concrete transformer $f^{\vec{\mathsf{r}}}$ in $\dot{\alpha}_{\vec{x}} \circ f^{\vec{\mathsf{r}}} \circ \dot{\gamma}_{\vec{x}}$ and then simplify to get an overapproximation $f^{\vec{x}}$.
  Then check the semi-commutation $f^{\vec{x}} \circ \dot{\alpha}_{\vec{x}} \sqsubseteq^{\vec{x}} \dot{\alpha}_{\vec{x}} \circ f^{\vec{\mathsf{r}}}$ (which implies $f^{\vec{\mathsf{r}}} \circ \dot{\gamma}_{\vec{x}} \sqsubseteq^{\vec{\alpha}} \dot{\gamma}_{\vec{x}} \circ f^{\vec{x}}$).
  (2) Expand the definition of $f^{\vec{\mathsf{r}}}$ in $\dot{\alpha}_{\vec{x}} \circ f^{\vec{\mathsf{r}}}(x)$ and overapproximate while pushing $\dot{\alpha}_{\vec{x}}$ toward the parameters x which yields a term of the form $t(\dot{\alpha}_{\vec{x}}(x))$ satisfying $\dot{\alpha}_{\vec{x}} \circ f^{\vec{\mathsf{r}}}(x) \sqsubseteq^{\vec{x}} t(\dot{\alpha}_{\vec{x}}(x))$ so that we can define $f^{\vec{x}}(y) = t(y)$ by letting $y = \dot{\alpha}_{\vec{x}}(x)$ (which implies $f^{\vec{\mathsf{r}}} \circ \dot{\gamma}_{\vec{x}} \sqsubseteq^{\vec{\alpha}} \dot{\gamma}_{\vec{x}} \circ f^{\vec{x}}$).

- We prefer the second strategy which, by experience, requires less calculations.

Cartesian semantics assignment

We can now define the cartesian abstract semantics assignment based upon the cartesian evaluation of arithmetic expressions.

Theorem (28.15, cartesian assignment)

$$\dot{\alpha}_{\vec{x}} \circ \mathrm{assign}^{\vec{r}}[\![\mathtt{x}, \mathtt{A}]\!] \quad \dot{\subseteq} \quad \mathrm{assign}^{\vec{x}}[\![\mathtt{x}, \mathtt{A}]\!] \circ \dot{\alpha}_{\vec{x}}$$

where $\mathrm{assign}^{\vec{x}}[\![\mathtt{x}, \mathtt{A}]\!]\overline{\rho} \quad \triangleq \quad \overline{\rho}[\mathtt{x} \leftarrow \mathscr{A}^{\vec{x}}[\![\mathtt{A}]\!]\overline{\rho}]$.

Proof of Theorem 28.15

$$
\begin{array}{lll}
 & \dot{\alpha}_{\vec{x}} \circ \mathrm{assign}^{\vec{r}}[\![x, A]\!]\overline{\rho} & \\
= & \dot{\alpha}_{\vec{x}}(\{\rho[x \leftarrow \mathscr{A}[\![A]\!]\ \rho] \mid \rho \in \overline{\rho}\}) & \text{def. (19.12) of } \mathrm{assign}^{\vec{r}}[\![\_,\_]\!] \\
= & y \in \mathbb{V} \mapsto \{\rho[x \leftarrow \mathscr{A}[\![A]\!]\ \rho](y) \mid \rho \in \overline{\rho}\} & \text{def. (28.1) of } \dot{\alpha}_{\vec{x}} \\
= & y \in \mathbb{V} \mapsto (\!|\ \overline{\rho} = \varnothing\ ?\ \varnothing\ |\ y = x\ ?\ \{\mathscr{A}[\![A]\!]\ \rho \mid \rho \in \overline{\rho}\}\ :\ \{\rho(y) \mid \rho \in \overline{\rho}\}\ |\!) & \\
 & & \text{def. (19.10) of environment assignment} \\
= & y \in \mathbb{V} \mapsto (\!|\ \overline{\rho} = \varnothing\ ?\ \varnothing\ |\ y = x\ ?\ \{\mathscr{A}[\![A]\!]\ \rho \mid \rho \in \overline{\rho}\}\ :\ \dot{\alpha}_{\vec{x}}(\overline{\rho})(y)\ |\!) & \text{def. (28.1) of } \dot{\alpha}_{\vec{x}} \\
\subseteq & y \in \mathbb{V} \mapsto (\!|\ \overline{\rho} = \varnothing\ ?\ \varnothing\ |\ y = x\ ?\ \mathscr{A}^{\vec{x}}[\![A]\!](\dot{\alpha}_{\vec{x}}(\overline{\rho}))\ :\ \dot{\alpha}_{\vec{x}}(\overline{\rho})(y)\ |\!) & \text{by Lemma 28.14} \\
= & (\!|\ \dot{\alpha}_{\vec{x}}(\overline{\rho}) = \dot{\varnothing}\ ?\ \dot{\varnothing}\ :\ \dot{\alpha}_{\vec{x}}(\overline{\rho})[x \leftarrow \mathscr{A}^{\vec{x}}[\![A]\!](\dot{\alpha}_{\vec{x}}(\overline{\rho}))]\ |\!) & \\
 & & \text{def. (19.10) of environment assignment and } \overline{\rho} = \varnothing \Leftrightarrow \dot{\alpha}_{\vec{x}}(\overline{\rho}) = \dot{\varnothing} \\
= & \dot{\alpha}_{\vec{x}}(\overline{\rho})[x \leftarrow \mathscr{A}^{\vec{x}}[\![A]\!](\dot{\alpha}_{\vec{x}}(\overline{\rho}))] & \text{since } \mathscr{A}^{\vec{x}}[\![A]\!](\dot{\varnothing}) = \varnothing \text{ implies } \dot{\varnothing}[x \leftarrow \mathscr{A}^{\vec{x}}[\![A]\!](\dot{\varnothing})] = \dot{\varnothing} \\
= & \mathrm{assign}^{\vec{x}}[\![x, A]\!](\dot{\alpha}_{\vec{x}}(\overline{\rho})) & \text{def. } \mathrm{assign}^{\vec{x}}[\![x, A]\!]\overline{\rho} \triangleq \overline{\rho}[x \leftarrow \mathscr{A}^{\vec{x}}[\![A]\!]\overline{\rho}]\ \square
\end{array}
$$

Structural cartesian
abstract reachability/forward
semantics of assignment

- In practice, $\mathbb{P}^\times = \wp(\mathbb{V})$ is large or infinite so a further abstraction $\gamma_\natural \in \langle \mathbb{P}^\natural, \sqsubseteq^\natural \rangle \leftrightarrows \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$ (where $\sqsubseteq^\times = \subseteq$) may be needed.
- This abstraction can be extended pointwise to $\dot{\gamma}_\natural \in \langle \mathbb{V} \to \mathbb{P}^\natural, \dot{\sqsubseteq}^\natural \rangle \leftrightarrows \langle \mathbb{V} \to \mathbb{P}^\times, \dot{\subseteq} \rangle$.

Cartesian abstract forward semantics of an arithmetic expression A

Define the abstract cartesian semantics of an expression A and an assignment statement x = A ; as follows ($\overline{P}, \overline{\rho} \in \mathbb{V} \to \mathbb{P}^\natural$)

$$
\begin{array}{rcll}
\circledcirc^\natural(\overline{P})\,\overline{\rho} & \triangleq & (\!|\, \overline{\rho} = \bot^\natural \;?\; \bot^\natural \;:\; \overline{P} \,|\!) & \text{if } \gamma_\natural(\bot^\natural) = \bot^\times, \ldots, \gamma_\natural(\bot^\times) = \varnothing, \text{ smash} \\
 & \triangleq & \overline{P} & \text{otherwise} \\
\mathscr{A}^\natural[\![1]\!]\,\overline{\rho} & \triangleq & \circledcirc^\natural(1^\natural)\,\overline{\rho} & (28.17) \\
\mathscr{A}^\natural[\![\mathtt{x}]\!]\,\overline{\rho} & \triangleq & \circledcirc^\natural(\overline{\rho}(\mathtt{x}))\,\overline{\rho} & \\
\mathscr{A}^\natural[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\,\overline{\rho} & \triangleq & \circledcirc^\natural(\mathscr{A}^\natural[\![\mathtt{A}_1]\!]\,\overline{\rho} \ominus^\natural \mathscr{A}^\natural[\![\mathtt{A}_2]\!]\,\overline{\rho})\,\overline{\rho} &
\end{array}
$$

Theorem 28.18 and Theorem 28.19 (Soundness abstract cartesian assignment) If

- $\mathscr{A}^{\times}[\![\mathtt{A}]\!]$ is an instance of (28.17) for $\langle \mathbb{P}^{\times}, \sqsubseteq^{\times} \rangle$ (including (28.13)),
- $\mathscr{A}^{\natural}[\![\mathtt{A}]\!]$ is an instance of (28.17) for $\langle \mathbb{P}^{\natural}, \sqsubseteq^{\natural} \rangle$,
- $\gamma_{\natural} \in \langle \mathbb{P}^{\natural}, \sqsubseteq^{\natural} \rangle \longrightarrow\!\!\!\!\!\nearrow \langle \mathbb{P}^{\times}, \sqsubseteq^{\times} \rangle$ is increasing,
- $1^{\times} \sqsubseteq^{\times} \gamma_{\natural}(1^{\natural})$, $\ominus^{\times}$ is $\sqsubseteq^{\times}$-argumentwise increasing, and
- $\forall X, Y \in \mathbb{P}^{\natural} \,.\, \gamma_{\natural}(X) \ominus^{\times} \gamma_{\natural}(Y) \sqsubseteq^{\times} \gamma_{\natural}(X \ominus^{\natural} Y)$

then

$$\mathscr{A}^{\times}[\![\mathtt{A}]\!] \circ \dot{\gamma}_{\natural} \quad \dot{\sqsubseteq}^{\times} \quad \dot{\gamma}_{\natural} \circ \mathscr{A}^{\natural}[\![\mathtt{A}]\!]$$

$$\mathrm{assign}^{\times}[\![\mathtt{x}, \mathtt{A}]\!] \circ \dot{\gamma}_{\natural} \quad \dot{\sqsubseteq}^{\times} \quad \dot{\gamma}_{\natural} \circ \mathrm{assign}^{\natural}[\![\mathtt{x}, \mathtt{A}]\!]$$

where

$$\mathrm{assign}^{\natural}[\![\mathtt{x}, \mathtt{A}]\!]\, \overline{\rho} \quad \triangleq \quad \overline{\rho}[\mathtt{x} \leftarrow \mathscr{A}^{\natural}[\![\mathtt{A}]\!]\overline{\rho}] \qquad (28.20) \quad \square$$

Remark (28.21)

- As shown by the proofs of Theorems 28.18 and 28.19, they are valid for $\mathbb{P}^\times = \wp(\mathbb{V})$ since (28.13) is an instance of (28.17).
- Moreover, the hypothesis that $\ominus$ is argumentwise increasing is only necessary in the concrete that is, when composing abstractions, for $\ominus^\times$, which follows from (28.13).

Cartesian static analysis of arithmetic expressions (II/II)

Structural accessibility/backward semantics of arithmetic expressions

Accessibility backward semantics of arithmetic expressions

- From a condition on an expression for a test to be true, we need to infer a condition on the variables of this expression for this test to be true.
- For example from $1 \leqslant x + 1 \leqslant 2$, we want to infer that $0 \leqslant x \leqslant 1$.
- For that purpose, we define the accessibility semantics of arithmetic expressions.

$$\begin{array}{rcl} \mathscr{A}^{-1}[\![\mathtt{A}]\!] & \in & \wp(\mathbb{V}) \to \wp(\mathbb{V} \to \mathbb{V}) \to \wp(\mathbb{V} \to \mathbb{V}) \\ \mathscr{A}^{-1}[\![\mathtt{A}]\!]\, \chi\, P & \triangleq & P \cap \mathrm{pre}[\mathscr{A}[\![\mathtt{A}]\!]]\chi \;=\; \{\rho \in P \mid \mathscr{A}[\![\mathtt{A}]\!]\rho \in \chi\} \end{array} \tag{28.22}$$

- $\mathscr{A}^{-1}[\![\mathtt{A}]\!]\, \chi\, P$ restricts the precondition P to those environments in which the arithmetic expression $\mathtt{A}$ may return a value in the set of values χ (considered as a postcondition).
- Example: $\mathscr{A}^{-1}[\![\mathtt{x + 1}]\!]\, (\overbrace{\{\nu \mid 1 \leqslant \nu \leqslant 2\}}^{\chi})\ \overbrace{\{\rho \mid \rho(\mathtt{x}) \leqslant 10\}}^{P} = \{\rho \mid 0 \leqslant \rho(\mathtt{x}) \leqslant 1\}$
- $\mathscr{A}^{-1}[\![\mathtt{A}]\!]\, \chi$ is a lower closure operator on the set $\mathbb{E}\mathtt{v}$ of environments.

Example (28.23)

- Assume the precondition $P = \{\langle x,\ y\rangle \mid 0 \leqslant x \leqslant 6 \wedge 2 \leqslant y \leqslant 7\}$.
- After the test $0 \leqslant \mathtt{x} + \mathtt{y} \leqslant 5$, the set of possible values of $x + y$ is $\chi = \{z \mid 0 \leqslant z \leqslant 5\}$.
- We have $\mathscr{A}^{-1}[\![\mathtt{A}]\!]\ \chi\ P = \{\langle x,\ y\rangle \mid 0 \leqslant x \leqslant 3 \wedge 2 \leqslant y \leqslant 5\}$ since otherwise $\max x + \min y > 5$ or $\min x + \max y > 5$.

The accessibility semantics of arithmetic expressions is expressed structurally by the following

Theorem (28.24)

$$\begin{aligned}
\mathscr{A}^{-1}[\![\mathtt{1}]\!]\ \chi\ P &= (\!|\ 1 \in \chi\ ?\ P\ :\ \varnothing\ |\!) \\
\mathscr{A}^{-1}[\![\mathtt{x}]\!]\ \chi\ P &= \{\rho \in P \mid \rho(\mathtt{x}) \in \chi\} \\
\mathscr{A}^{-1}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\ \chi\ P &= \{\rho \in P \mid (\mathscr{A}[\![\mathtt{A}_1]\!]\ \rho - \mathscr{A}[\![\mathtt{A}_2]\!]\ \rho) \in \chi\}
\end{aligned}$$

□

Structural cartesian accessibility/backward semantics of arithmetic expressions

Accessibility backward semantics of arithmetic expressions

- We look for a cartesian overapproximation

$$\mathscr{A}^{\vec{\mathbb{X}}_1}[\![\mathtt{A}]\!] \quad \in \quad \wp(\mathbb{V}) \to (\mathbb{V} \to \wp(\mathbb{V})) \to (\mathbb{V} \to \wp(\mathbb{V}))$$

  of $\mathscr{A}^{-1}[\![\mathtt{A}]\!]$.
- Given a binary operation $b \in \mathbb{V} \times \mathbb{V} \to \mathbb{V}$ define

$$\begin{array}{rcl} b^{\vec{\mathbb{X}}_1} & \in & \wp(\mathbb{V}) \to (\wp(\mathbb{V}) \times \wp(\mathbb{V})) \to (\wp(\mathbb{V}) \times \wp(\mathbb{V})) \\ b^{\vec{\mathbb{X}}_1}\ \chi\ \langle \chi_1, \chi_2 \rangle & \triangleq & \langle \{v_1 \in \chi_1 \mid \exists v_2 \in \chi_2 \,.\, (v_1\ b\ v_2) \in \chi\}, \\ & & \quad \{v_2 \in \chi_2 \mid \exists v_1 \in \chi_1 \,.\, (v_1\ b\ v_2) \in \chi\} \rangle \end{array} \tag{28.26}$$

- $b^{\vec{\mathbb{X}}_1}\ \chi$ is a lower closure operator on $\wp(\mathbb{V}) \times \wp(\mathbb{V})$.

Example 2 Continuing Example 28.23, $+^{\vec{\mathbb{X}}_1}\ [0,5]\ \langle [0,6],\ [2,7] \rangle = \langle [0,3],\ [2,5] \rangle$. □

- Then, by calculational design, we get [P. Cousot, 1999]

Cartesian accessibility semantics of an arithmetic expression A

$$\mathscr{A}^{\vec{\asymp}_1}[\![1]\!]\,\chi\,\overline{\rho} \triangleq (\!|\, 1 \in \chi \,?\, \overline{\rho} : \dot{\varnothing} \,|\!) \qquad (\dot{\varnothing} \triangleq x \in \mathbb{V} \mapsto \varnothing) \tag{28.28}$$

$$\mathscr{A}^{\vec{\asymp}_1}[\![x]\!]\,\chi\,\overline{\rho} \triangleq (\!|\, \overline{\rho}(x) \cap \chi \neq \varnothing \,?\, \overline{\rho}[x \leftarrow \overline{\rho}(x) \cap \chi] : \dot{\varnothing} \,|\!)$$

$$\mathscr{A}^{\vec{\asymp}_1}[\![A_1 - A_2]\!]\,\chi\,\overline{\rho} \triangleq \text{let } \langle \chi_1, \chi_2 \rangle = \ominus^{\vec{\asymp}_1}\,\chi\,\langle \mathscr{A}^{\vec{\asymp}}[\![A_1]\!]\overline{\rho},\ \mathscr{A}^{\vec{\asymp}}[\![A_2]\!]\overline{\rho} \rangle \text{ in } \mathscr{A}^{\vec{\asymp}_1}[\![A_1]\!]\,\chi_1\,\overline{\rho} \,\dot{\cap}\, \mathscr{A}^{\vec{\asymp}_1}[\![A_2]\!]\,\chi_2\,\overline{\rho}$$

Note: $b^{\vec{\asymp}_1}$ where $b = -$ is denoted $\ominus^{\asymp_1}$.

- $\mathscr{A}^{\vec{\asymp}_1}[\![A]\!]\,\chi$ is a lower closure operator on $\mathbb{V} \to \wp(\mathbb{V})$ and
- $\mathscr{A}^{\vec{\asymp}_1}[\![A]\!]\,\chi$ is $\dot{\subseteq}$-increasing in χ.

Theorem (28.29) $\dot{\alpha}_{\vec{\asymp}} \circ \mathscr{A}^{-1}[\![A]\!]\,\chi \mathrel{\dot{\subseteq}} \mathscr{A}^{\vec{\asymp}_1}[\![A]\!]\,\chi \circ \dot{\alpha}_{\vec{\asymp}}$.

Structural cartesian abstract accessibility/backward semantics of arithmetic expressions

- As noticed in Section **28.4.3**, in practice, $\mathbb{P}^{\times} = \wp(\mathbb{V})$ is large or infinite so we consider a further cartesian abstraction $\gamma_{\natural} \in \langle \mathbb{P}^{\natural}, \sqsubseteq^{\natural} \rangle \longrightarrow\!\!\!\!\!\rightarrow \langle \mathbb{P}^{\times}, \sqsubseteq^{\times} \rangle$ extended pointwise to $\dot{\gamma}_{\natural} \in \langle \mathbb{V} \to \mathbb{P}^{\natural}, \dot{\sqsubseteq}^{\natural} \rangle \longrightarrow\!\!\!\!\!\rightarrow \langle \mathbb{V} \to \mathbb{P}^{\times}, \dot{\sqsubseteq}^{\times} \rangle$.

Cartesian accessibility semantics of an arithmetic expression A

$$
\begin{array}{rcl}
\mathscr{A}^{\natural_1}[\![1]\!]\,\chi\,\overline{\rho} & \triangleq & (\!|\, 1^{\natural} \sqcap^{\natural} \chi \neq \bot^{\natural} \;?\; \overline{\rho} \;:\; \bot^{\natural} \,|\!) \\
\mathscr{A}^{\natural_1}[\![\mathtt{x}]\!]\,\chi\,\overline{\rho} & \triangleq & (\!|\, \overline{\rho}(\mathtt{x}) \sqcap^{\natural} \chi \neq \bot^{\natural} \;?\; \overline{\rho}[\mathtt{x} \leftarrow \overline{\rho}(\mathtt{x}) \sqcap^{\natural} \chi] \;:\; \bot^{\natural} \,|\!) \\
\mathscr{A}^{\natural_1}[\![\mathtt{A}_1 - \mathtt{A}_2]\!]\,\chi\,\overline{\rho} & \triangleq & \text{let } \langle \chi_1, \chi_2 \rangle = \ominus^{\natural_1}\,\chi\,\langle \mathscr{A}^{\natural}[\![\mathtt{A}_1]\!]\overline{\rho},\ \mathscr{A}^{\natural}[\![\mathtt{A}_2]\!]\overline{\rho} \rangle \text{ in} \\
& & \quad \mathscr{A}^{\natural_1}[\![\mathtt{A}_1]\!]\,\chi_1\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\mathscr{A}^{\natural_1}[\![\mathtt{A}_2]\!]\,\chi_2\,\overline{\rho}
\end{array}
\qquad (28.30)
$$

- $\mathscr{A}^{\natural_1}[\![\mathtt{A}]\!]\,\chi$ is a lower closure operator on $\mathbb{V} \to \mathbb{P}^{\natural}$ and
- $\mathscr{A}^{\natural_1}[\![\mathtt{A}]\!]\,\chi$ is $\sqsubseteq^{\natural}$-increasing in χ.

Theorem (28.31) If

- $\mathscr{A}^{\dot{\times}_1}$ is an instance of (28.30) for $\langle \mathbb{P}^{\times}, \sqsubseteq^{\times} \rangle$,
- $\mathscr{A}^{\dot{\alpha}_1}$ is an instance of (28.30) for $\langle \mathbb{P}^{\alpha}, \sqsubseteq^{\alpha} \rangle$,
- $\gamma_{\alpha} \in \langle \mathbb{P}^{\alpha}, \sqsubseteq^{\alpha} \rangle \xrightarrow{\sqcap} \langle \mathbb{P}^{\times}, \sqsubseteq^{\times} \rangle$ preserves finite meets,
- is strict $(\forall P \in \mathbb{P}^{\alpha} \,.\, (P = \bot^{\alpha}) \Rightarrow (\gamma_{\alpha}(P) = \bot^{\times}))$,
- $\gamma_{\alpha}(1^{\alpha}) = 1^{\times}$,
- the hypotheses of Theorem 28.18 hold,
- $(\Theta^{\dot{\times}_1}\ \chi)$ is argumentwise increasing, and
- $\Theta^{\dot{\times}_1}\ \gamma_{\alpha}(\chi)\ \langle \gamma_{\alpha}(P_1), \gamma_{\alpha}(P_2) \rangle \dot{\subseteq} \dot{\gamma}_{\alpha}(\Theta^{\dot{\alpha}_1}\ \chi\ \langle P_1, P_2 \rangle)$

then

$$\mathscr{A}^{\dot{\times}_1}[\![\mathsf{A}]\!]\ \gamma_{\alpha}(\chi) \circ \dot{\gamma}_{\alpha} \quad \dot{\sqsubseteq}^{\times} \quad \dot{\gamma}_{\alpha} \circ \mathscr{A}^{\dot{\alpha}_1}[\![\mathsf{A}]\!]\ \chi. \qquad \square$$

Remark (28.32)

- Following *Remark* 28.21, (28.28) is an instance of (28.30)
- the proof of Theorem 28.31 does not depend on the fact that $\mathbb{P}^\times = \wp(\mathbb{V})$ so is valid for any cartesian abstraction provided the hypotheses are expressed for $\mathbb{P}^\times$ instead of $\wp(\mathbb{V})$.

Cartesian static analysis of boolean expressions

Structural cartesian
reachability/forward semantics of tests

- The cartesian abstract semantics of a conditional or an iteration statement involves the cartesian abstract semantics of boolean expressions defined as follows.
- Given a relation operation $r \in \mathbb{V} \times \mathbb{V} \to \mathbb{B}$, $x \in \chi_1$. and $y \in \chi_2$, $\langle \chi_1', \chi_2' \rangle = r^{\vec{\times}} \langle \chi_1, \chi_2 \rangle$ is the subset of values of $x \in \chi_1' \subseteq \chi_1$ and $y \in \chi_2' \subseteq \chi_2$ for which the relation $x \, r \, y$ may hold.

Example 3 If $x \in [1,4]$ and $y \in [0,3]$ then $x < y$ implies $x < \max\{y \mid y \in [0,3]\} = 3$ and $1 = \min\{x \mid x \in [1,4]\} < y$ so $x \in [1,2]$ and $y \in [2,3]$. Therefore $r^{\vec{\times}}\langle [1,4], [0,3]\rangle = \langle [1,2], [2,3]\rangle$ when $r = <$. □

We define

$$
\begin{array}{rcl}
r^{\vec{\times}}, \overline{r}^{\vec{\times}} & \in & (\wp(\mathbb{V}) \times \wp(\mathbb{V})) \to (\wp(\mathbb{V}) \times \wp(\mathbb{V})) \\
r^{\vec{\times}} \langle \chi_1, \chi_2 \rangle & \triangleq & \langle \{v_1 \in \chi_1 \mid \exists v_2 \in \chi_2 \,.\, v_1 \, r \, v_2\}, \{v_2 \in \chi_2 \mid \exists v_1 \in \chi_1 \,.\, v_1 \, r \, v_2\} \rangle \\
\overline{r}^{\vec{\times}} \langle \chi_1, \chi_2 \rangle & \triangleq & \langle \{v_1 \in \chi_1 \mid \exists v_2 \in \chi_2 \,.\, \neg(v_1 \, r \, v_2)\}, \{v_2 \in \chi_2 \mid \exists v_1 \in \chi_1 \,.\, \neg(v_1 \, r \, v_2)\} \rangle
\end{array}
$$

Structural cartesian reachability semantics of tests B

$$
\begin{array}{rcl}
\mathrm{test}^{\vec{\times}}[\![\mathtt{A}_1 < \mathtt{A}_2]\!]\,\overline{\rho} & \triangleq & \mathrm{let}\ \langle A_1,\ A_2\rangle = \circledcirc^{\vec{\times}}\ \langle \mathscr{A}^{\vec{\times}}[\![\mathtt{A}_1]\!]\,\overline{\rho},\ \mathscr{A}^{\vec{\times}}[\![\mathtt{A}_2]\!]\,\overline{\rho}\rangle\ \mathrm{in} \\
 & & \quad \mathscr{A}^{\times_1}[\![\mathtt{A}_1]\!]\,A_1\,\overline{\rho}\,\dot{\cap}\,\mathscr{A}^{\times_1}[\![\mathtt{A}_2]\!]\,A_2\,\overline{\rho} \\
\overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{A}_1 < \mathtt{A}_2]\!]\,\overline{\rho} & \triangleq & \mathrm{let}\ \langle A_1,\ A_2\rangle = \overline{\circledcirc}^{\times}\ \langle \mathscr{A}^{\vec{\times}}[\![\mathtt{A}_1]\!]\,\overline{\rho},\ \mathscr{A}^{\vec{\times}}[\![\mathtt{A}_2]\!]\,\overline{\rho}\rangle\ \mathrm{in} \\
 & & \quad \mathscr{A}^{\times_1}[\![\mathtt{A}_1]\!]\,A_1\,\overline{\rho}\,\dot{\cap}\,\mathscr{A}^{\times_1}[\![\mathtt{A}_0]\!]\,A_2\,\overline{\rho} \\
\mathrm{test}^{\vec{\times}}[\![\mathtt{B}_1\ \mathtt{nand}\ \mathtt{B}_1]\!]\,\overline{\rho} & \triangleq & (\mathrm{test}^{\vec{\times}}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\cap}\,\overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{B}_2]\!]\,\overline{\rho}) \\
 & & \dot{\cup}\,(\overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\cap}\,\mathrm{test}^{\vec{\times}}[\![\mathtt{B}_2]\!]\,\overline{\rho}) \\
 & & \dot{\cup}\,(\overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\cap}\,\overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{B}_2]\!]\,\overline{\rho}) \\
\overline{\mathrm{test}}^{\vec{\times}}[\![\mathtt{B}_1\ \mathtt{nand}\ \mathtt{B}_2]\!]\,\overline{\rho} & \triangleq & \mathrm{test}^{\vec{\times}}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\cap}\,\mathrm{test}^{\vec{\times}}[\![\mathtt{B}_2]\!]\,\overline{\rho}
\end{array}
\tag{28.34}
$$

Note: $r^{\vec{\times}}$ (resp. $\overline{r}^{\vec{\times}}$) is denoted $\circledcirc^{\vec{\times}}$ (resp. $\overline{\circledcirc}^{\vec{\times}}$) when $r = <$.

Theorem (28.35, cartesian test) $\dot{\alpha}_{\vec{\mathtt{x}}} \circ \mathtt{test}^{\vec{r}}[\![\mathtt{B}]\!] \mathrel{\dot{\subseteq}} \mathtt{test}^{\vec{\times}}[\![\mathtt{B}]\!] \circ \dot{\alpha}_{\vec{\mathtt{x}}}$ and $\dot{\alpha}_{\vec{\mathtt{x}}} \circ \overline{\mathtt{test}}^{\vec{r}}[\![\mathtt{B}]\!] \mathrel{\dot{\subseteq}} \overline{\mathtt{test}}^{\vec{\times}}[\![\mathtt{B}]\!] \circ \dot{\alpha}_{\vec{\mathtt{x}}}$.

- $\dot{\alpha}_{\vec{\mathtt{x}}} \circ \mathtt{test}^{\vec{r}}[\![\mathtt{A}_1 < \mathtt{A}_2]\!] \mathrel{\dot{\subseteq}} \mathtt{test}^{\times}[\![\mathtt{A}_1 < \mathtt{A}_2]\!] \circ \dot{\alpha}_{\vec{\mathtt{x}}}$.
- $\mathtt{test}^{\times}[\![\mathtt{B}]\!]$ is a lower closure operator.

Structural cartesian abstract abstract reachability/forward semantics of tests

- We now consider a further cartesian abstraction $\gamma_{\natural} \in \langle \mathbb{P}^{\natural}, \sqsubseteq^{\natural} \rangle \xrightarrow{\sqcap} \langle \mathbb{P}^{\times}, \sqsubseteq^{\times} \rangle$ of the cartesian abstract domain and extend it pointwise to $\dot{\gamma}_{\natural} \in \langle \mathcal{V} \to \mathbb{P}^{\natural}, \dot{\sqsubseteq}^{\natural} \rangle \xrightarrow{\sqcap} \langle \mathcal{V} \to \mathbb{P}^{\times}, \dot{\subseteq} \rangle$.
- The cartesian abstract semantics of tests

cartesian abstract semantics of tests $\mathtt{B}$

$$\begin{aligned}
\mathrm{test}^{\natural}[\![\mathtt{A}_1 < \mathtt{A}_2]\!]\,\overline{\rho} &\triangleq \mathrm{let}\ \langle A_1, A_2\rangle = \circledcirc^{\natural}\,\langle \mathscr{A}^{\natural}[\![\mathtt{A}_1]\!]\,\overline{\rho},\ \mathscr{A}^{\natural}[\![\mathtt{A}_2]\!]\,\overline{\rho}\rangle\ \mathrm{in} \\
&\qquad \mathscr{A}^{\natural_1}[\![\mathtt{A}_1]\!]\,A_1\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\mathscr{A}^{\natural_1}[\![\mathtt{A}_2]\!]\,A_2\,\overline{\rho} \qquad (28.38)\\
\overline{\mathrm{test}}^{\natural}[\![\mathtt{A}_1 < \mathtt{A}_2]\!]\,\overline{\rho} &\triangleq \mathrm{let}\ \langle A_1, A_2\rangle = \overline{\circledcirc}^{\natural}\,\langle \mathscr{A}^{\natural}[\![\mathtt{A}_1]\!]\,\overline{\rho},\ \mathscr{A}^{\natural}[\![\mathtt{A}_2]\!]\,\overline{\rho}\rangle\ \mathrm{in} \\
&\qquad \mathscr{A}^{\natural_1}[\![\mathtt{A}_1]\!]\,A_1\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\mathscr{A}^{\natural_1}[\![\mathtt{A}_0]\!]\,A_2\,\overline{\rho} \\
\mathrm{test}^{\natural}[\![\mathtt{B}_1\ \mathtt{nand}\ \mathtt{B}_1]\!]\,\overline{\rho} &\triangleq (\mathrm{test}^{\natural}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\overline{\mathrm{test}}^{\natural}[\![\mathtt{B}_2]\!]\,\overline{\rho}) \\
&\quad \dot{\sqcup}^{\natural}\,(\overline{\mathrm{test}}^{\natural}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\mathrm{test}^{\natural}[\![\mathtt{B}_2]\!]\,\overline{\rho}) \\
&\quad \dot{\sqcup}^{\natural}\,(\overline{\mathrm{test}}^{\natural}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\overline{\mathrm{test}}^{\natural}[\![\mathtt{B}_2]\!]\,\overline{\rho}) \\
\overline{\mathrm{test}}^{\natural}[\![\mathtt{B}_1\ \mathtt{nand}\ \mathtt{B}_2]\!]\,\overline{\rho} &\triangleq \mathrm{test}^{\natural}[\![\mathtt{B}_1]\!]\,\overline{\rho}\,\dot{\sqcap}^{\natural}\,\mathrm{test}^{\natural}[\![\mathtt{B}_2]\!]\,\overline{\rho}
\end{aligned}$$

Theorem 28.39 (abstract cartesian test) If

- $\ominus^\times$ is argumentwise increasing,
- $\ominus^\times \langle \gamma_\natural(X), \gamma_\natural(Y)\rangle \mathrel{\dot{\sqsubseteq}}^\times \dot\gamma_\natural(\ominus^\natural \langle X, Y\rangle))$, and
- $\gamma_\natural$ preserves finite glbs

then $\mathsf{test}^\times[\![\mathtt{B}]\!] \circ \dot\gamma_\natural \mathrel{\dot{\sqsubseteq}}^\times \dot\gamma_\natural \circ \mathsf{test}^\natural[\![\mathtt{B}]\!]$ and $\overline{\mathsf{test}}^\times[\![\mathtt{B}]\!] \circ \dot\gamma_\natural \mathrel{\dot{\sqsubseteq}}^\times \dot\gamma_\natural \circ \overline{\mathsf{test}}^\natural[\![\mathtt{B}]\!]$.

Remark (28.40)

- The proof of Theorem 28.39 shows that the theorem holds for an abstraction of the cartesian semantics as well as for abstractions of abstractions of this cartesian semantics.
- The hypotheses are on the concrete semantics hence, by composition of abstractions, need only hold for the cartesian semantics, which they do.
- $\mathsf{test}^{\natural}[\![\mathtt{B}]\!]$ is increasing and reductive.

Cartesian abstract domain
of abstract value properties

- Theorems 28.15, 28.29, and 28.35 show that all cartesian abstract domains have the same mathematical structure while Theorems 28.18, 28.19, 28.31, and 28.39 show that this mathematical structure is preserved by further cartesian abstractions.
- They all have the same structure

$$\mathbb{D}^\natural \quad \triangleq \quad \langle \mathbb{P}^\natural, \sqsubseteq^\natural, \bot^\natural, \top^\natural, \sqcup^\natural, \sqcap^\natural, 1^\natural, \ominus^\natural, \ominus^{\natural_1}, \circledcirc^\natural, \overline{\circledcirc}^\natural \rangle \qquad (28.42)$$

They are all abstractions of the cartesian collecting domain

$$\langle \wp(\mathbb{V}), \subseteq, \varnothing, \mathbb{V}, \cup, \cap, \{1\}, \ominus, \ominus^{\rightleftarrows_1}, \circledcirc^{\rightleftarrows_1}, \overline{\circledcirc}^{\rightleftarrows_1} \rangle$$

for a concretization $\gamma_\natural \in \mathbb{P}^\natural \xrightarrow{\curvearrowright} \wp(\mathbb{V})$ satisfying the hypotheses of Theorems **??**, 28.31, and 28.39 (which are satisfyied by the cartesian collecting semantics).

Cartesian abstract domain of abstract reachability properties

- The abstract interpreter of Chapter **21** can be used with the cartesian abstract domain of abstract reachability properties of the form

$$\mathbb{D}^{\dot{\natural}} \quad \triangleq \quad \langle \mathcal{V} \to \mathbb{P}^{\natural}, \dot{\sqsubseteq}^{\natural}, \dot{\bot}^{\natural}, \dot{\sqcup}^{\natural}, \mathsf{assign}^{\natural}[\![\mathtt{x}, \mathtt{A}]\!], \mathsf{test}^{\natural}[\![\mathtt{B}]\!], \overline{\mathsf{test}}^{\natural}[\![\mathtt{B}]\!] \rangle \quad (28.43)$$

for the concretizations $\dot{\gamma}_{\natural} \in (\mathcal{V} \to \mathbb{P}^{\natural}) \dot{\longrightarrow} (\mathcal{V} \to \wp(\mathbb{V}))$ and $\dot{\gamma}_{\vec{\natural}} \in (\mathcal{V} \to \wp(\mathbb{V})) \dot{\longrightarrow} \wp(\mathcal{V} \to \mathbb{V})$.

Theorem 4 28.44 (Well-definedness and soundness of the cartesian static analysis) The cartesian abstract domain $\mathbb{D}^{\dot{\natural}}$ (28.43) is well-defined according to Definition 21.1 so the abstract interpreter $\widehat{\mathcal{S}}^{\dot{\natural}}[\![\mathtt{S}]\!]$ is well-defined and a sound abstraction of the assertional forward reachability semantics $\mathcal{S}^{\vec{r}}[\![\mathtt{S}]\!]$ for any program component $\mathtt{S} \in \mathbb{P}\mathbb{c}$. □

Proof of Theorem 28.44 By Theorems 28.18, 28.19, 28.31, and 28.39, the cartesian abstract domain $\mathbb{D}^{\dot{\alpha}}$ is well-defined according to Definition 21.1 and an approximate domain abstraction according to Definition 27.1-I. We conclude, by Theorem 21.16 and Theorem 27.4, that the abstract interpreter of 21.3—21.13 of Chapter **21**, instantiated with the cartesian abstract domain $\mathbb{D}^{\dot{\alpha}}$ of abstract reachability properties of (28.43) is a sound abstraction of the assertional forward reachability semantics $\mathcal{S}^{\vec{r}}[\![\mathsf{s}]\!]$ of Chapter **19**. □

Remark 5

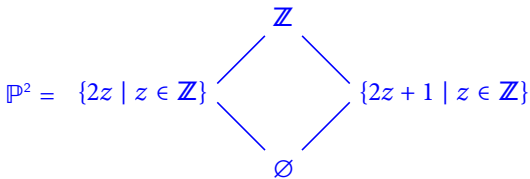
- Observe that the concrete/abstract domains are *universal algebræ* or, briefly *algebræ*, that a set S equipped with finitary operations on S *i.e.* taking a finite number of parameters which is 0 for constants [Grätzer, 2008].
- All operations of the cartesian algebræ $\mathbb{D}^{\dot{\sharp}}$ are defined in term of the operations of the cartesian algebra $\mathbb{D}^{\sharp}$ so there is a functor $\dot{\mathfrak{F}}^{\times}[\![\mathcal{V}]\!]$ mapping the cartesian algebræ $\mathbb{D}^{\sharp}$ to the cartesian algebræ $\mathbb{D}^{\dot{\sharp}}$ where the operations are defined in Theorems 28.18, 28.19, 28.31, and 28.39.
- Some programming languages directly support such algebræ and functors like OCaml modules and module functors [Leroy, Doligez, Frisch, Garrigue, Rémy, and Vouillon, 2020].
- The abstract domain $\mathbb{D}^{\dot{\sharp}}$ can be efficiently implemented as a functor taking as parameter the module implementing $\mathbb{D}^{\sharp}$.
- The abstract interpreter is then itself a functor taking as parameter the module implementing $\mathbb{D}^{\dot{\sharp}}$.

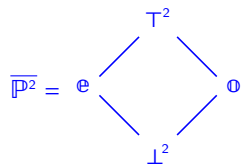
□

Examples of cartesian abstractions

Parity abstraction

- The cartesian parity abstract domain $\mathbb{D}^{\dot{2}} \triangleq \langle \mathbb{V} \to \mathbb{P}^2, \dot{\sqsubseteq^2}, \dot{\bot^2}, \dot{\sqcup^2}, \mathsf{assign}_2[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^{\dot{2}}[\![\mathsf{B}]\!], \overline{\mathsf{test}}^{\dot{2}}[\![\mathsf{B}]\!] \rangle$ is the pointwise extension of the parity value abstract domain $\langle \mathbb{P}^2, \sqsubseteq^2, \bot^2, \top^2, \sqcup^2, \sqcap^2 \rangle$ below.





- For the cartesian reachability semantics of arithmetic expressions $\mathsf{assign}_2[\![\mathsf{x}, \mathsf{A}]\!]$, we use (28.17) with $\alpha_2(\{1\}) = \mathbb{o}$ and

x	$\mathbb{e}$	$\mathbb{e}$	$\mathbb{o}$	$\mathbb{o}$	$\_$	$\bot^2/\top^2$
y	$\mathbb{e}$	$\mathbb{o}$	$\mathbb{e}$	$\mathbb{o}$	$\bot^2/\top^2$	$\_$
$x \ominus^2 y$	$\mathbb{e}$	$\mathbb{o}$	$\mathbb{o}$	$\mathbb{e}$	$\bot^2/\top^2$	$\bot^2/\top^2$

- For the cartesian accessibility semantics $\mathscr{A}^{2_1}[\![\mathtt{A}]\!]$ of an arithmetic expression A, we use (28.30) with

χ	$p1$	$p2$	$\Theta^{2_1}\,\chi\,\langle p1,\ p2\rangle$
$\top^2$	$\_$	$\_$	$\langle p1,\ p2\rangle$
$\mathbb{e}$	$\mathbb{e}$	$\mathbb{e}$	$\langle \mathbb{e},\ \mathbb{e}\rangle$
$\mathbb{e}$	$\mathbb{o}$	$\mathbb{o}$	$\langle \mathbb{o},\ \mathbb{o}\rangle$
$\mathbb{o}$	$\mathbb{e}$	$\mathbb{o}$	$\langle \mathbb{e},\ \mathbb{o}\rangle$
$\mathbb{o}$	$\mathbb{o}$	$\mathbb{e}$	$\langle \mathbb{o},\ \mathbb{e}\rangle$
$\_$	$\_$	$\_$	$\langle \bot^2,\ \bot^2\rangle$

- For tests $\mathtt{test}^2[\![\mathtt{B}]\!]$, the equality implies that the parities are the same. The other comparison tests provide no information on parity.
- Example(`(at,atP,af,afP,es,br,brP)`)

```
<l1:x=e, y=e; l4:x=o, y=e; ff; l0:x=_|_, y=_|_>  Prog:
<l1:x=e, y=e; l2:x=o, y=e; ff; l0:x=_|_, y=_|_>     l1: x = 1;
<l2:x=o, y=e; l4:x=o, y=e; ff; l0:x=_|_, y=_|_>     (while l2: (0 < 1)
<l3:x=o, y=e; l2:x=o, y=e; ff; l0:x=_|_, y=_|_>        l3: x = (x + 2); )
                                                    l4:
```

Sign abstraction

- The cartesian sign abstract domain $\mathbb{D}^\sharp \triangleq \langle \mathbb{V} \to \mathbb{P}^\pm, \sqsubseteq^\sharp, \bot^\sharp, \sqcup^\sharp, \mathsf{assign}_\pm[\![\mathtt{x}, \mathtt{A}]\!], \mathsf{test}^\sharp[\![\mathtt{B}]\!], \overline{\mathsf{test}}^\sharp[\![\mathtt{B}]\!] \rangle$ is the pointwise extension of the sign value abstract domain $\langle \mathbb{P}^\pm, \sqsubseteq^\pm, \bot^\pm, \top^\pm, \sqcup^\pm, \sqcap^\pm \rangle$ considered in Section **3.12**.
- The assignment is $A[x \leftarrow \mathscr{A}^\pm[\![\mathtt{A}]\!]A]$ where the analysis $\mathscr{A}^\pm[\![\mathtt{A}]\!]A$ expression $\mathtt{A}$ applies the rule of signs as designed in Section **3.20**.
- A simple handling of boolean expressions would be case analysis

$$
\begin{array}{rcl}
\mathsf{test}^\sharp[\![\mathtt{x == 0}]\!]A & \triangleq & (\!| A(\mathtt{x}) \sqcap^\pm (=0) = \bot_\pm \mathbin{?} \mathtt{x} \mapsto \bot_\pm \mathbin{:} A[x \leftarrow (=0)] |\!) \\
\mathsf{test}^\sharp[\![\mathtt{x == y}]\!]A & \triangleq & (\!| A(\mathtt{x}) \sqcap^\pm A(\mathtt{y}) = \bot_\pm \mathbin{?} \mathtt{x} \mapsto \bot_\pm \\
 & & \mathbin{:} A[x \leftarrow A(\mathtt{x}) \sqcap^\pm A(\mathtt{y})][y \leftarrow A(\mathtt{x}) \sqcap^\pm A(\mathtt{y})] |\!) \\
\mathsf{test}^\sharp[\![\mathtt{x > 0}]\!]A & \triangleq & (\!| A(\mathtt{x}) \sqcap^\pm (>0) = \bot_\pm \mathbin{?} \mathtt{x} \mapsto \bot_\pm \mathbin{:} A[x \leftarrow A(\mathtt{x}) \sqcap^\pm (>0)] |\!) \\
\cdots & \cdots & \cdots \\
\mathsf{test}^\sharp[\![\mathtt{A}]\!]A & \triangleq & A
\end{array}
$$

- The treatment of tests in Theorem 28.39 is more precise. The operators $\circledcirc^{\pm_1}$ and $\overline{\circledcirc}^{\pm_1}$ are given in [P. Cousot, 1999].

Constancy abstraction

- The cartesian constant abstract domain $\mathbb{D}^{\dot{c}} \triangleq \langle \mathcal{V} \to \mathbb{P}^c, \dot{\sqsubseteq^c}, \dot{\bot^c}, \dot{\top^c}, \dot{\sqcup^c}, \mathsf{assign}^{\dot{c}}_c[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^{\dot{c}}[\![\mathsf{B}]\!], \overline{\mathsf{test}}^{\dot{c}}[\![\mathsf{B}]\!] \rangle$ is the pointwise extension of the constant value abstract domain $\mathbb{D}^c \triangleq \langle \mathbb{P}^c, \sqsubseteq^c, \bot^c, \top^c, \sqcup^c, \mathsf{assign}^c_c[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^c[\![\mathsf{B}]\!], \overline{\mathsf{test}}^c[\![\mathsf{B}]\!] \rangle$ of Exercise 3.43.
- For assignments and tests, $\bot^c$ and $\dot{\top^c}$ are absorbant.
- Otherwise the assignments and tests involve only constants and can be evaluated in the concrete.

Conclusion

Conclusion

- We have designed a collecting semantics for cartesian abstract interpretation by abstraction of the reachability semantics.
- Although the given examples where for finitary abstract domains, this is not mandatory (contrary to the understanding of static analysis where values are replaced by symbolic abstract values [Kildall, 1973; Naur, 1965; Sintzoff, 1972; Wegbreit, 1975]).
- Interval analysis [P. Cousot and R. Cousot, 1976] is an example of infinitary cartesian abstraction.
- Cartesian abstraction is the basis of SLAM [Ball, Podelski, and Rajamani, 2003], a widely advertised static analyzer of device drivers lacking precision and scalability.
- It is also used in Astrée [Bertrane, P. Cousot, R. Cousot, Feret, Mauborgne, Miné, and Rival, 2015] for analyzing control-command software, but in conjunction with many complementary relational scalable abstract domains for precision.

Bibliography I

Ball, Thomas, Andreas Podelski, and Sriram K. Rajamani (2003). "Boolean and Cartesian abstraction for model checking C programs". *STTT* 5.1, pp. 49–58.

Bertrane, Julien, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, and Xavier Rival (2015). "Static Analysis and Verification of Aerospace Software by Abstract Interpretation". *Foundations and Trends in Programming Languages* 2.2-3, pp. 71–190.

Cousot, Patrick (1999). "The Calculational Design of a Generic Abstract Interpreter". In: M. Broy and R. Steinbrüggen, eds. *Calculational System Design*. NATO ASI Series F. IOS Press, Amsterdam.

Cousot, Patrick and Radhia Cousot (1976). "Static determination of dynamic properties of programs". In: *Proceedings of the Second International Symposium on Programming*. Dunod, Paris, France, pp. 106–130.

Bibliography II

Descartes, René (1637). *La Géométrie*. Leyde. URL: https://gallica.bnf.fr/ark:/12148/bpt6k29040s.image.

Grätzer, George (2008). *Universal Algebra*. 2nd ed. Springer.

Kildall, Gary A. (1973). "A Unified Approach to Global Program Optimization". In: *POPL*. ACM Press, pp. 194–206.

Leroy, Xavier, Damien Doligez, Alain Frisch, Jacques Garrigue, Didier Rémy, and Jérôme Vouillon (Feb. 2020). "The OCaml system, release 4.10, Documentation and user's manual". Copyright © 2020 Institut National de Recherche en Informatique et en Automatique. URL: http://caml.inria.fr/pub/docs/manual-ocaml/.

Naur, Peter (Sept. 1965). "Checking of operand types in ALGOL compilers". *BIT Numerical Mathematics* 5, pp. 151–163.

Bibliography III

Sintzoff, Michel (1972). "Calculating Properties of Programs by Valuations on Specific Models". In: *Proceedings of ACM Conference on Proving Assertions About Programs*. ACM, pp. 203–207.

Wegbreit, Ben (1975). "Property Extraction in Well-Founded Property Sets". *IEEE Trans. Software Eng.* 1.3, pp. 270–285.

Home work

Read Ch. **28** "Abstract cartesian semantics" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you