Principles of Abstract Interpretation

MIT press

Ch. 36, Reduced Product

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-36--reduced-product-PrAbsInt.pdf

Chapter 36

Ch. 36, Reduced Product (1/5)

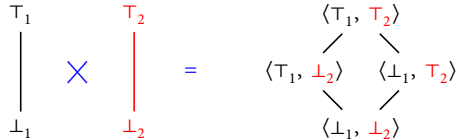
We have split our review of chapter 36 into five videos

This first video is about

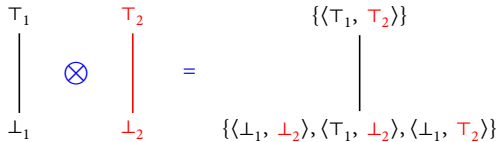
- the direct and reduced products, informally

Direct product and reduced product

- The *direct product* of several static analyses is the conjunction of the separately computed analyses.



- The *reduced product* of several static analyses [P. Cousot and R. Cousot, 1979] computes in the conjunction of their abstract domains.



- In that case, information on program executions captured by one domain can be used to improve the precision of the information provided by other abstract domains. This is called a *meaning-preserving reduction*.
- As shown in chapter 29, reductions can be iterated to obtain more precise and still sound analyzes.

Direct product, section 36.1

Direct product

- The direct product of abstract domains can be used to perform *simultaneous independent analyzes* of a program.
- The set of properties of the direct product is the cartesian product of the component abstract properties.
- The concretization is the conjunction (meet) of the concretizations for each abstract domain
- The transformers are performed componentwise without interactions.

Definition (36.1, Direct product) Let

$$\overline{\mathbb{D}}^i \triangleq \langle \overline{\mathbb{P}}^i, \sqsubseteq^i, \bot^i, \sqcup^i, \mathsf{assign}_i[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^i[\![\mathsf{B}]\!], \overline{\mathsf{test}}^i[\![\mathsf{B}]\!] \rangle,$$

$i \in \Delta$, Δ finite, be several abstract domains.

Each $\overline{\mathbb{D}}^i$ abstracts a concrete domain $\mathbb{D} \triangleq \langle \mathbb{P}, \sqsubseteq, \bot, \sqcap, \sqcup, \mathsf{assign}[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}[\![\mathsf{B}]\!], \overline{\mathsf{test}}[\![\mathsf{B}]\!] \rangle$ by a concretization $\gamma^i \in \overline{\mathbb{P}}^i \nearrow\!\!\longrightarrow \mathbb{P}$ (or a Galois connection).

Their *direct product* is the abstract domain

$\mathbb{D}^\times \triangleq \bigtimes_{i\in\Delta} \overline{\mathbb{D}}^i \triangleq \langle \mathbb{P}^\times, \sqsubseteq^\times, \bot^\times, \sqcap^\times, \sqcup^\times, \mathsf{assign}_\times[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^\times[\![\mathsf{B}]\!], \overline{\mathsf{test}}^\times[\![\mathsf{B}]\!] \rangle$

The abstract operations are combined componentwise, for example

- $\vec{P} \in \mathbb{P}^\times \triangleq \{\prod_{i\in\Delta} P_i \mid \forall i \in \Delta \,.\, P_i \in \overline{\mathbb{P}}^i\}$,
- $\prod_{i\in\Delta} P_i \sqsubseteq^\times \prod_{i\in\Delta} P'_i \triangleq \bigwedge_{i\in\Delta} P_i \sqsubseteq^i P'_i$,
- $\mathsf{test}^\times[\![\mathsf{B}]\!] \prod_{i\in\Delta} P_i \triangleq \prod_{i\in\Delta} \mathsf{test}^i[\![\mathsf{B}]\!] P_i$, etc.

The concretization is $\gamma^\times \in \mathbb{P}^\times \nearrow\!\!\longrightarrow \mathbb{P}$ defined by $\gamma^\times(\prod_{i\in\Delta} P_i) \triangleq \bigsqcap_{i\in\Delta} \gamma^i(P_i)$.

Direct product

- The direct product can be used to perform the conjunction of several independent static analyzes.
- Because abstract transformers are applied component-wise, there is no interaction between the abstract domains $\overline{\mathbb{D}}^i$, $i \in \Delta$,
- So, the concretization of the static analysis of programs by the abstract interpreter of chapter 21 with the direct product $\mathbb{D}^\times$ yields exactly the same result as the conjunction of the results produced by the abstract interpreter of chapter 21 with each abstract domain $\overline{\mathbb{D}}^i$, $i \in \Delta$ separately.

example 36.2

- Consider the separate sign analysis (of section 28.8.2) and parity analysis (of section 28.8.1) of the following program.

program	sign of x	parity of x	conjunction of separate analyzes
`x = -1977 ;`	<0	$\mathbb{O}$	$<0 \wedge \mathbb{O}$
`/* loop invariant */`	$\top_\pm$	$\mathbb{O}$	$\top_\pm \wedge \mathbb{O}$
`while (x < 0) {`	<0	$\mathbb{O}$	$<0 \wedge \mathbb{O}$
`  x = x + 2 ;`	$\top_\pm$	$\mathbb{O}$	$\top_\pm \wedge \mathbb{O}$
`}`	$\geqslant 0$	$\mathbb{O}$	$>0 \wedge \mathbb{O}$
`x = x - 1 ;`	$\top_\pm$	$\mathbb{E}$	$\top_\pm \wedge \mathbb{E}$

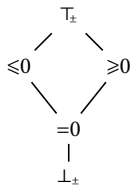
- Their conjunction reduces the loop exit invariant from $(\geqslant 0 \wedge \mathbb{O})$ to $(>0 \wedge \mathbb{O})$ since x being positive and odd cannot be 0.
- However the program exit invariant $(\top_\pm \wedge \mathbb{E})$ is not improved.

Reduced product, informally, section 36.2

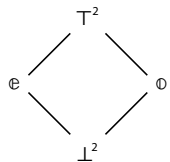
Example exercise 36.4, reduction of parity and simple sign analysis

The reduction sign and parity goes as follows.

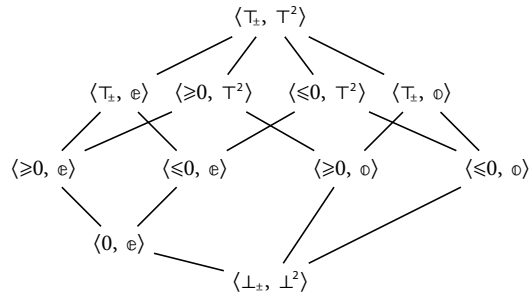
$$\langle \bot_\pm, \_ \rangle \to \langle \bot_\pm, \bot^2 \rangle \qquad \langle 0, \top^2 \rangle \to \langle 0, \mathbb{e} \rangle$$
$$\langle \_, \bot^2 \rangle \to \langle \bot_\pm, \bot^2 \rangle \qquad \langle 0, \mathbb{o} \rangle \to \langle \bot_\pm, \bot^2 \rangle$$
$$\langle \leqslant 0, \mathbb{o} \rangle \to \langle < 0, \mathbb{o} \rangle \qquad \langle \geqslant 0, \mathbb{o} \rangle \to \langle > 0, \mathbb{o} \rangle$$



Sign



Parity



Reduced product

Example 36.3, Reduced product of sign and parity I

- Continuing example 36.2, the two analyses are performed simultaneously and the reduction is performed on the fly during these analyses.

program	sign of x	parity of x	reduced product
`x = -1977 ;`	$<0 \rightarrow <0$	$\mathbb{O} \rightarrow \mathbb{O}$	$<0 \wedge \mathbb{O}$
`/* loop invariant */`	$\top_{\pm} \rightarrow \top_{\pm}$	$\mathbb{O} \rightarrow \mathbb{O}$	$\top_{\pm} \wedge \mathbb{O}$
`while (x < 0) {`	$<0 \rightarrow <0$	$\mathbb{O} \rightarrow \mathbb{O}$	$<0 \wedge \mathbb{O}$
`  x = x + 2 ;`	$\top_{\pm} \rightarrow \top_{\pm}$	$\mathbb{O} \rightarrow \mathbb{O}$	$\top_{\pm} \wedge \mathbb{O}$
`}`	$\geqslant 0 \rightarrow >0$	$\mathbb{O} \rightarrow \mathbb{O}$	$>0 \wedge \mathbb{O}$
`x = x - 1 ;`	$\geqslant 0 \rightarrow \geqslant 0$	$\mathbb{e} \rightarrow \mathbb{e}$	$\geqslant 0 \wedge \mathbb{e}$

- The reduction $\langle \leqslant 0, \mathbb{O} \rangle \rightarrow \langle <0, \mathbb{O} \rangle$ yields >0 for signs and $\mathbb{O}$ unchanged for parity.
- Then the assignment `x = x - 1 ;` yields $\geqslant 0$ for signs and $\mathbb{e}$ for parity which is more precise than the conjunction $(\top_{\pm} \wedge \mathbb{e})$ after the separate analyses.

Reduced product

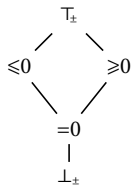
- The reduced product of abstract domains can be used to perform *simultaneous dependent* analyzes of a program where the abstract domains share common information during the analysis.
- The reduced product of static analyzes consist in computing them simultaneously with a reduction at each step.
- This is in general much easier to develop than designing a new analysis combining the two and more precise than computing them separately.
- The reduction of example 36.3 is "strong" in that it is the most precise possible.
- An example of "weak" reduction would be the *smash product* that extend an infimum to all components of the product i.e.

$$\langle x_1, \ldots, x_{i-1}, \bot^i, x_{i+1}, \ldots, x_n \rangle \to \langle \bot^1, \ldots, \bot^{i-1}, \bot^i, \bot^{i+1}, \ldots, \bot^n \rangle$$

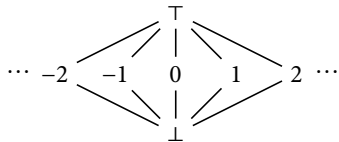
when $\gamma^\times(\bot^i) = \bot$ is the empty set of reachable states.

Example 36.5 Reduced product of simple sign and constant

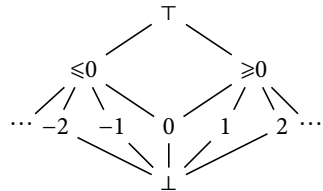
Draw the lattice of properties which is the reduction of simple sign analysis of exercise 36.4 and the constant analysis of exercise 3.45.



Sign



Constancy



Reduced product

Reduced product

- The reduced product of two abstractions

$$\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_\natural}{\overset{\gamma_\natural}{\leftrightarrows}} \langle \mathbb{P}^\natural, \overline{\sqsubseteq}^\natural \rangle \otimes \langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_\sharp}{\overset{\gamma_\sharp}{\leftrightarrows}} \langle \overline{\mathbb{P}}^\sharp, \overline{\sqsubseteq}^\sharp \rangle \triangleq$$
$$\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_\otimes}{\overset{\gamma_\otimes}{\leftrightarrows}} \langle \{ \langle \alpha_\natural(\gamma_\natural(\overline{P}^\natural) \sqcap \gamma_\sharp(\overline{P}^\sharp)),\ \alpha_\sharp(\gamma_\natural(\overline{P}^\natural) \sqcap \gamma_\sharp(\overline{P}^\sharp)) \rangle \mid \overline{P}^\natural \in \mathbb{P}^\natural \wedge \overline{P}^\sharp \in \overline{\mathbb{P}}^\sharp \},\ \overline{\sqsubseteq}^\natural \times \overline{\sqsubseteq}^\sharp \rangle$$

  (where $\overline{\sqsubseteq}^\natural \times \overline{\sqsubseteq}^\sharp$ is componentwise) brings into each analysis the information of the other analysis which is expressible in this analysis.
- The property $\langle \overline{P}^\natural, \overline{P}^\sharp \rangle$ meaning $(\gamma_\natural(\overline{P}^\natural) \sqcap \gamma_\sharp(\overline{P}^\sharp))$ is reduced to $\langle \alpha_\natural(\gamma_\natural(\overline{P}^\natural) \sqcap \gamma_\sharp(\overline{P}^\sharp)),\ \alpha_\sharp(\gamma_\natural(\overline{P}^\natural) \sqcap \gamma_\sharp(\overline{P}^\sharp)) \rangle$.
- The information of one abstract domain pertinent to the other abstract domain is collected by this other abstract domain.
- For example the information $\overline{P}^\natural$ of abstract domain $\mathbb{P}^\natural$ pertinent to $\overline{\mathbb{P}}^\sharp$ is collected by $\overline{\mathbb{P}}^\sharp$ thanks to $\alpha_\sharp(\gamma_\natural(\overline{P}^\natural) \sqcap \gamma_\sharp(\overline{P}^\sharp))$.

This concludes our informal study

- the direct and reduced products

from chapter 36, "Reduced Product"

The End

Principles of Abstract Interpretation

MIT press

Ch. 36, Reduced Product

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-36--reduced-product-PrAbsInt.pdf

Chapter 36

Ch. 36, Reduced Product (2/5)

In this second video, we study

- the formal definition of the reduced product

Reduced product, formally, section 36.3

Reduced product

- To improve the precision of the direct product, the reduced product was defined [P. Cousot and R. Cousot, 1979] so that each analysis benefits from the information brought by the other analyses.
- We will introduce three equivalent definition of the reduced product.

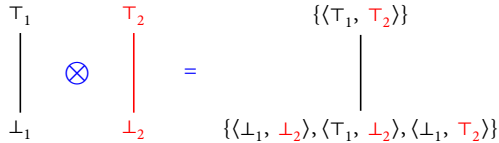
Definition 1 of $\otimes$: equivalence of properties with same meaning

Definition (36.7, Reduced product (I)) Let $\mathbb{D} \triangleq \langle \mathbb{P}, \sqsubseteq, \bot, \sqcap, \sqcup, \mathsf{assign}[\![\mathsf{x},\mathsf{A}]\!], \mathsf{test}[\![\mathsf{B}]\!], \overline{\mathsf{test}}[\![\mathsf{B}]\!] \rangle$ be a concrete domain. Let $\overline{\mathbb{D}}^i \triangleq \langle \overline{\mathbb{P}}^i, \sqsubseteq^i, \bot^i, \sqcup^i, \mathsf{assign}_i[\![\mathsf{x},\mathsf{A}]\!], \mathsf{test}^i[\![\mathsf{B}]\!], \overline{\mathsf{test}}^i[\![\mathsf{B}]\!] \rangle$, $i \in \Delta$, Δ finite, be abstract domains with increasing concretization $\gamma_i \in \overline{\mathbb{P}}_i \xrightarrow{\nearrow} \mathbb{P}$. Let $\mathbb{D}^\times = \bigtimes_{i\in\Delta} \overline{\mathbb{D}}^i$ be their direct product with concretization $\gamma^\times$.

Their *reduced product* is $\mathbb{D}^\otimes \triangleq \bigotimes_{i\in\Delta} \overline{\mathbb{D}}^i \triangleq \langle \mathbb{P}^\otimes, \sqsubseteq^\otimes, \bot^\otimes, \sqcup^\otimes, \mathsf{assign}_\otimes[\![\mathsf{x},\mathsf{A}]\!], \mathsf{test}^\otimes[\![\mathsf{B}]\!], \overline{\mathsf{test}}^\otimes[\![\mathsf{B}]\!] \rangle$ where the reduced properties $\mathbb{P}^\otimes \triangleq \mathbb{P}^\times/_{\equiv^\otimes}$ are the equivalence classes of the equivalence relation $(\vec{P} \equiv^\otimes \vec{Q}) \triangleq (\gamma^\times(\vec{P}) = \gamma^\times(\vec{Q}))$ on the direct product $\mathbb{P}^\times$ and all operations are extended to these equivalence classes $\mathbb{P}^\otimes = \{[\vec{P}]_{\equiv^\otimes} \mid \vec{P} \in \mathbb{P}^\times\}$ of $\equiv^\otimes$ as follows.

- $\forall \vec{P} \in \mathbb{P}^\times \,.\, \gamma^\otimes([\vec{P}]_{\equiv^\otimes}) = \gamma^\times(\vec{P})$;
- $[\vec{P}]_{\equiv^\otimes} \sqsubseteq^\times [\vec{Q}]_{\equiv^\otimes} \triangleq \exists \vec{P}' \in [\vec{P}]_{\equiv^\otimes} \,.\, \exists \vec{Q}' \in [\vec{Q}]_{\equiv^\otimes} \,.\, \vec{P}' \sqsubseteq^\times \vec{Q}'$;
- $\bot^\otimes \triangleq [\bot]_{\equiv^\otimes}$;
- $\bigsqcup_{k\in K}^\otimes [\vec{P}_k]_{\equiv^\otimes} \triangleq [\bigsqcup_{k\in K}^\times \vec{P}_k]_{\equiv^\otimes}$;
- $\mathsf{assign}_\otimes[\![\mathsf{x},\mathsf{A}]\!][\vec{P}]_{\equiv^\otimes} \triangleq [\mathsf{assign}_\times[\![\mathsf{x},\mathsf{A}]\!]\vec{P}]_{\equiv^\otimes}$;
- $\mathsf{test}^\otimes[\![\mathsf{B}]\!][\vec{P}]_{\equiv^\otimes} \triangleq [\mathsf{test}^\times[\![\mathsf{B}]\!]\vec{P}]_{\equiv^\otimes}$;
- $\overline{\mathsf{test}}^\otimes[\![\mathsf{B}]\!][\vec{P}]_{\equiv^\otimes} \triangleq [\overline{\mathsf{test}}^\times[\![\mathsf{B}]\!]\vec{P}]_{\equiv^\otimes}$.

- Notice that the definitions are independent of the choices of the representatives (e.g. $\vec{P}$) of the equivalence classes (e.g. $[\vec{P}]_{\equiv_\otimes}$).
- In practice the equivalence classes are implemented using a representent chosen by a meaning-preserving reduction operation (see section 36.3.4).
- Example (smash product):



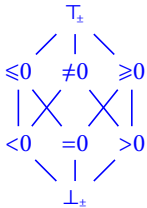
Definition 2 of $\otimes$: glb in the lattice of abstract domains

section 36.3.1, The hierarchy (poset/complete lattice) of abstract domains

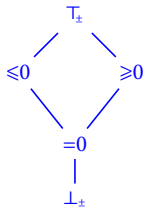
- We can compare the expressiveness of abstract properties by defining abstract properties $\overline{\mathbb{P}}_1$ to be more expressive/precise than $\overline{\mathbb{P}}_2$ whenever any property exactly expressible by $\overline{\mathbb{P}}_2$ is also expressible by $\overline{\mathbb{P}}_1$[1].
- Two sets of abstract properties are equivalent when they are equally expressive.

Example of lattice of abstract domains

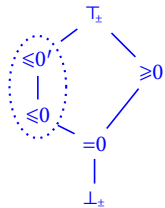
- The lattice of signs (a) of section 3.12 is strictly more expressive than the lattice (b) of exercise 36.4 since all sign properties of (b) can be expressed by (a) while "strictly positive" in (a) must be overapproximated by "positive or zero" in (b).
- Both (a) and (b) are incomparable with (c) since (c) lacks "positive or zero" found in (a) and (b) while (a) and (b) both lack "strictly greater than one" found in (c).
- The two lattices (b) and (b′) are equally expressive since they have the same concretization ($\gamma(\leqslant 0') = \gamma(\leqslant 0)$).



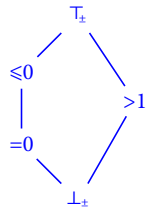
(a)



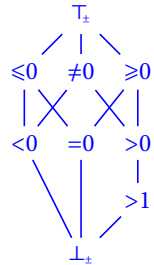
(b)



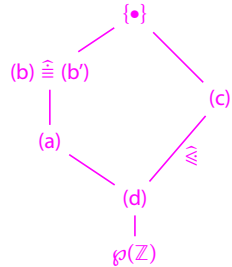
(b′)



(c)



(d)



lattice of abstract domains

Definition 1 (36.10, Precision of abstractions) Let $\langle \mathbb{P}, \sqsubseteq \rangle$ be a complete lattice of concrete properties [b].

Let $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i \rangle$, $i \in \{1, 2\}$, be abstract properties with concretization $\gamma_i \in \overline{\mathbb{P}}_i \to \mathbb{P}$.

We say that $\overline{\mathbb{P}}_2$ is *less precise* (also *less expressive*, *less refined*, etc...) *than* $\overline{\mathbb{P}}_1$ (written $\overline{\mathbb{P}}_1 \mathrel{\hat{\leqslant}} \overline{\mathbb{P}}_2$ [c]) whenever $\gamma_2(\overline{\mathbb{P}}_2) \subseteq \gamma_1(\overline{\mathbb{P}}_1)$ [d].

They are *equivalent* whenever $\gamma_1(\overline{\mathbb{P}}_1) = \gamma_2(\overline{\mathbb{P}}_2)$ (written $\overline{\mathbb{P}}_1 \mathrel{\hat{=}} \overline{\mathbb{P}}_2$). □

b. for example $\langle \mathbb{P}, \sqsubseteq \rangle = \langle \wp(\wp(\mathbb{T}^{+\infty})), \subseteq \rangle$ in chapter 8, "Program Properties" or $\langle \mathbb{P}, \sqsubseteq \rangle = \langle \wp(\mathbb{E}\mathbb{v}^{\varrho}) \to (\mathbb{L} \to \wp(\mathbb{E}\mathbb{v}^{\varrho})), \ddot{\subseteq} \rangle$ in chapter 19, "Structural Forward Reachability Semantics."

c. $\hat{\leqslant}$-smaller abstract domains are more precise/expressive while $\hat{\leqslant}$-larger abstract domains are less precise/expressive, like $\{\bot, \top\} \mathrel{\hat{\leqslant}} \{\top\}$.

d. where the right image of a set X by a function f is $f(X) = \{f(x) \mid x \in X\}$.

- Any domain of abstract properties $\overline{\mathbb{P}}$ can express a subset $\gamma(\overline{\mathbb{P}})$ of the concrete properties $\mathbb{P}$.
- Two $\hat{\dot{\equiv}}$-equivalent sets of abstract properties $\overline{\mathbb{P}}_1$ and $\overline{\mathbb{P}}_2$ are just different encoding of some element of the complete lattice $\langle \wp(\mathbb{P}), \supseteq \rangle$.
- So the set of all sets of abstract properties $\overline{\mathbb{P}}$ quotiented by $\hat{\dot{\equiv}}$ and ordered by precision $\hat{\dot{\leqslant}}$ is isomorphic to the complete lattice $\langle \wp(\mathbb{P}), \supseteq \rangle$ [P. Cousot and R. Cousot, 1979].
- When the abstractions are defined by Galois connections $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle \overline{\mathbb{P}}_1, \sqsubseteq_1 \rangle$ and $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle \overline{\mathbb{P}}_2, \sqsubseteq_2 \rangle$, we have $\overline{\mathbb{P}}_1 \mathrel{\hat{\dot{\leqslant}}} \overline{\mathbb{P}}_2 \Leftrightarrow \gamma_1 \circ \alpha_1(\mathbb{P}) \supseteq \gamma_2 \circ \alpha_2(\mathbb{P})$ [P. Cousot and R. Cousot, 1979].

Proof of $\overline{\mathbb{P}}_1 \mathrel{\widehat{\lessdot}} \overline{\mathbb{P}}_2 \Leftrightarrow \gamma_1 \circ \alpha_1(\mathbb{P}) \supseteq \gamma_2 \circ \alpha_2(\mathbb{P})$

— $\overline{\mathbb{P}}_1 \mathrel{\widehat{\lessdot}} \overline{\mathbb{P}}_2$

$\Rightarrow \forall \overline{P}_2 \in \overline{\mathbb{P}}_2 \,.\, \exists \overline{P}_1 \in \overline{\mathbb{P}}_1 \,.\, \gamma_1(\overline{P}_1) = \gamma_2(\overline{P}_2)$ ⟅def. $\widehat{\lessdot}$⟆

$\Rightarrow \forall P_2 \in \mathbb{P} \,.\, \exists \overline{P}_1 \in \overline{\mathbb{P}}_1 \,.\, \gamma_1(\overline{P}_1) = \gamma_2(\alpha_2(P_2))$ ⟅since $\alpha_2(P_2) \in \overline{\mathbb{P}}_2$⟆

$\Rightarrow \forall P_2 \in \mathbb{P} \,.\, \exists \overline{P}_1 \in \overline{\mathbb{P}}_1 \,.\, \gamma_1 \circ \alpha_1 \circ \gamma_1(\overline{P}_1) = \gamma_2 \circ \alpha_2(P_2)$

⟅$\gamma_1 \circ \alpha_1 \circ \gamma_1 = \gamma_1$ in Galois connection and def. $\circ$⟆

$\Rightarrow \forall P_2 \in \mathbb{P} \,.\, \exists P_1 \in \mathbb{P} \,.\, \gamma_1 \circ \alpha_1(P_1) = \gamma_2 \circ \alpha_2(P_2)$ ⟅taking $P_1 = \gamma_1(\overline{P}_1)$⟆

$\Rightarrow \gamma_2 \circ \alpha_2(\mathbb{P}) \subseteq \gamma_1 \circ \alpha_1(\mathbb{P})$ ⟅def. $\subseteq$⟆

— Conversely, for all $\overline{P}_2 \in \overline{\mathbb{P}}_2$ then $\gamma_2(\overline{P}_2) \in \mathbb{P}$ so

$\exists P_1 \in \mathbb{P} \,.\, \gamma_1 \circ \alpha_1(P_1) = \gamma_2 \circ \alpha_2(\gamma_2(\overline{P}_2)) = \gamma_2(\overline{P}_2)$ ⟅hyp. and $\gamma_2 \circ \alpha_2 \circ \gamma_2 = \gamma_2$ in GC⟆

$\Rightarrow \exists \overline{P}_1 \in \overline{\mathbb{P}}_1 \,.\, \gamma_1(\overline{P}_1) = \gamma_2(\overline{P}_2)$ ⟅choosing $\overline{P}_1 = \alpha_1(P_1)$⟆

$\Rightarrow \overline{\mathbb{P}}_1 \mathrel{\widehat{\lessdot}} \overline{\mathbb{P}}_2$ ⟅def. $\widehat{\lessdot}$⟆

section 36.3.2, The reduced product is the greatest lower bound in the poset of abstract domains (closed by intersection)

We show that the reduced product is the greatest lower bound (glb) for $\hat{\leqslant}$. By definition of the glb, the reduced product is the most imprecise abstract domain which is more precise than all domains in the product.

Definition (36.12. Closure by intersection) An abstract domain $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ with concretization $\gamma \in \overline{\mathbb{P}} \longrightarrow \mathbb{P}$ into a meet semi-lattice (resp. complete lattice) $\langle \mathbb{P}, \sqsubseteq, \sqcap \rangle$ is *closed by finite (resp. infinite) intersection* if and only if $\forall P, Q \in \overline{\mathbb{P}} \ . \ \exists R \in \overline{\mathbb{P}} \ . \ \gamma(R) = \gamma(P) \sqcap \gamma(Q)$ (resp. $\forall \mathscr{P} \in \wp(\overline{\mathbb{P}}) \ . \ \exists R \in \overline{\mathbb{P}} \ . \ \gamma(R) = \bigsqcap \gamma(\mathscr{P})$).

When considering only abstract domains that are closed by finite intersection, the reduced product can equivalently be understood as the greatest lower bound in the complete lattice of abstract domains, up to the equivalence $\hat{\equiv}$.

Theorem (36.14, Equivalent definition of the reduced product (II)) Let the meet semi-lattice $\langle \mathbb{P}, \sqsubseteq, \top, \sqcap \rangle$ be concrete properties;
Let $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i, \top_i \rangle$, $i \in \Delta$, Δ finite, be abstract properties with increasing concretization $\gamma_i \in \overline{\mathbb{P}}_i \xrightarrow{\nearrow} \mathbb{P}$ and supremum $\top_i$ such that $\gamma_i(\top_i) = \top$.

The reduced product $\langle \mathbb{P}^\times/_{\equiv^\otimes}, \sqsubseteq^\otimes, [\vec{\top}]_{\equiv^\otimes} \rangle$ is the greatest lower bound of the $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i \rangle$, $i \in \Delta$ in that it is

- more precise than $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$, $i \in \Delta$,
- less precise than any other $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$, which is closed by finite intersection and more precise than all the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$, $i \in \Delta$.

If $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i, \top_i \rangle$, $i \in \Delta$ are closed by finite intersection then their reduced product $\langle \mathbb{P}^\times/_{\equiv^\otimes}, \sqsubseteq^\otimes, [\vec{\top}]_{\equiv^\otimes} \rangle$ is the unique such domain of abstract properties (up to the equivalence $\hat{\equiv}$).

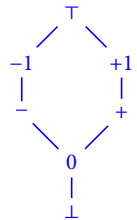
Definition 3 of $\otimes$: reduction of equivalent properties

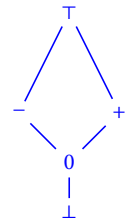
section 36.3.3, Abstract domain reduction

- Different abstract domains $\overline{\mathbb{P}}_1 \mathrel{\hat{\dot{=}}} \overline{\mathbb{P}}_2$ with the same expressive power may yield different abstract properties which, after iteration, may yield sound but quite different results.
- In particular, this is the case when the best transformer is difficult to compute algorithmically, so that a strict over-approximation $\overline{\mathscr{F}}[\![\mathsf{P}]\!] \dot{\supset} \alpha \circ \mathscr{F}[\![\mathsf{P}]\!] \circ \gamma$ has to be used instead.
- In such a case, reduction may be useful.

example 36.16

- Consider the abstraction of $\langle \wp(\mathbb{Z}), \subseteq \rangle$ by the complete lattice $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ such that

$\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle \triangleq$ 

$\langle \rho_\gamma(\overline{\mathbb{P}}), \overline{\sqsubseteq} \rangle \triangleq$ 

  where $\overline{\mathbb{P}} \triangleq \{\bot, 0, +, +1, -, -1, \top\}$, $\bot \sqsubset 0 \sqsubset + \sqsubset +1 \sqsubset \top$ and $0 \sqsubset - \sqsubset -1 \sqsubset \top$ with $\gamma(+) = \gamma(+1) = \{z \in \mathbb{Z} \mid z \geqslant 0\}$ and $\gamma(-) = \gamma(-1) = \{z \in \mathbb{Z} \mid z \leqslant 0\}$.

- The positive and negative properties have distinct but equivalent encodings in the abstract.
- The two transformers $f_1(0) = f_1(+) = +$, $f_1(+1) = \top$ and $f_2(0) = +$, $f_2(+) = +1$, $f_2(+1) = \top$ are equivalent in the concrete in that $\forall \overline{P} \in \mathbb{P} \,.\, \gamma(f_1(\overline{P})) = \gamma(f_2(\overline{P}))$
- but their composition is not since $\gamma(f_1(f_1(f_1(0)))) = \gamma(+) \neq \gamma(\top) = \gamma(f_2(f_2(f_2(0))))$.

- Another example is the reduction of the direct product of abstract domains into their reduced product.

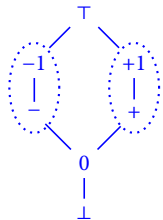
Example 2 (36.17) Consider the direct product of sign and parity in section 36.2

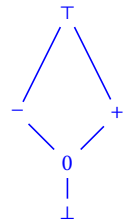
program	sign of x	parity of x	direct product
`x = −1977 ;`	$<0 \to <0$	$\mathbb{O} \to \mathbb{O}$	$<0 \wedge \mathbb{O}$
`/* loop invariant */`	$\top_\pm \to \top_\pm$	$\mathbb{O} \to \mathbb{O}$	$\top_\pm \wedge \mathbb{O}$
`while (x < 0) {`	$<0 \to <0$	$\mathbb{O} \to \mathbb{O}$	$<0 \wedge \mathbb{O}$
`  x = x + 2 ;`	$\top_\pm \to \top_\pm$	$\mathbb{O} \to \mathbb{O}$	$\top_\pm \wedge \mathbb{O}$
`}`	$\geqslant 0 \to >0$	$\mathbb{O} \to \mathbb{O}$	$>0 \wedge \mathbb{O}$
`x = x − 1 ;`	$\geqslant 0 \to \geqslant 0$	$\mathbb{E} \to \mathbb{E}$	$\top_\pm \wedge \mathbb{E}$

with a reduction $\langle \geqslant 0, \mathbb{O} \rangle \to \langle >0, \mathbb{O} \rangle$.
Then the assignment `x = x − 1 ;` yields $\geqslant 0$ for signs and $\mathbb{E}$ for parity which is more precise than the conjunction $(\top_\pm \wedge \mathbb{E})$ after the separate analyses. □

example 36.18

- The reduction of an abstract domain consists in eliminating the redundant abstract properties by putting them in normal/canonical form.
- Continuing example 36.16,

$\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle \triangleq$ 

$\langle \rho_\gamma(\overline{\mathbb{P}}), \overline{\sqsubseteq} \rangle \triangleq$ 

let us define the reduction $\rho_\gamma(a) \triangleq \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a')\}$ such that $\rho_\gamma(+1) = +$, $\rho_\gamma(-1) = -$ and otherwise $\rho_\gamma(a) = a$.

- The reduced abstract domain is $\rho_\gamma(\overline{\mathbb{P}}) = \{\bot, 0, +, -, \top\}$ where the redundant abstract properties $+1$ and -1 have been eliminated.

Theorem (36.19, Reduction Operator) Let $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ where $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq}, \overline{\bot}, \overline{\top}, \overline{\sqcup}, \overline{\sqcap} \rangle$ is a complete lattice. Define

$$\rho_\gamma(a) \triangleq \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a')\}$$

then ρ_γ is a lower closure (reductive, increasing and idempotent) on $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ and

$$\langle \mathbb{P}, \sqsubseteq \rangle \underset{\rho_\gamma \circ \alpha}{\overset{\gamma}{\leftrightarrows}} \langle \rho_\gamma(\overline{\mathbb{P}}), \overline{\sqsubseteq} \rangle .$$

Definition (36.20, Meaning-preserving Map/Reduction) Let the poset $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ be an abstract domain with concretization $\gamma \in \overline{\mathbb{P}} \nrightarrow \mathbb{P}$ into the concrete poset $\langle \mathbb{P}, \sqsubseteq \rangle$.

A *meaning-preserving map* is $\rho \in \overline{\mathbb{P}} \to \overline{\mathbb{P}}$ such that $\forall \overline{P} \in \overline{\mathbb{P}} \,.\, \gamma(\rho(\overline{P})) = \gamma(\overline{P})$.

The map is a *reduction* if and only if $\forall \overline{P} \in \overline{\mathbb{P}} \,.\, \rho(\overline{P}) \,\overline{\sqsubseteq}\, \overline{P}$.

Lemma (36.21) The composition of finitely many meaning-preserving reductions is a meaning-preserving reduction.

Proof By recurrence. For the induction step, observe that
$\gamma \circ (\rho_1 \circ \rho_2) = (\gamma \circ \rho_1) \circ \rho_2 = \gamma \circ \rho_2 = \gamma$ and $\forall \overline{P} \in \overline{\mathbb{P}} \,.\, (\rho_1 \circ \rho_2)(\overline{P}) = \rho_1(\rho_2(\overline{P})) \,\overline{\sqsubseteq}\, \rho_2(\overline{P}) \,\overline{\sqsubseteq}\, \overline{P}$. □

The following theorem shows that the reduction ρ_γ is meaning-preserving that is does not change the expressiveness of the reduced abstract properties.

Theorem (36.22) With the hypotheses of theorem 36.19, ρ_γ is meaning-preserving, $\gamma = \gamma \circ \rho_\gamma$.

- As shown by example 36.16,
  - abstract domains and transformers may have equivalent concretizations,
  - the equivalent but more precise abstract properties may propagate through several transformers
  - the resulting transformed properties and fixpoint computations maybe more precise in the concrete.
- Notice also that an implementation of the reduction of an abstract domain $\overline{\mathbb{P}}$ does not need considerable modifications of the implementation of $\overline{\mathbb{P}}$.
- The reduction operator ρ_γ may simply be applied before and after the operations of abstract domain $\overline{\mathbb{P}}$ (although maybe not after a widening/narrowing since the reduction might introduce divergences, see section 36.4.5).

section 36.3.4, The reduced product is the meaning-preserving reduction of the direct product

- The reduced product of abstract domains $\overline{\mathbb{P}}_i$, $i \in \Delta$ can be encoded by a reduction of the direct product $\prod_{i \in \Delta} \overline{\mathbb{P}}_i$ using a meaning-preserving reduction operator $\vec{\rho}$ mapping any element of the direct product to the smallest representative of its equivalence class.
- This yields a more constructive definition of reduction and later leads to algorithms to perform or approximate this reduction.

Theorem (36.24, Equivalent definition of the reduced product (III)) Let $\langle \mathbb{P}, \sqsubseteq \rangle$ be a poset; Let $\forall i \in \Delta$, Δ finite, each $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i, \overline{\bot}_i, \overline{\top}_i, \overline{\sqcup}_i, \overline{\sqcap}_i \rangle$ be a complete lattice such that $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_i}{\overset{\gamma_i}{\leftrightarrows}} \langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$.

Let $\langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$ be the direct product of the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$, $i \in \Delta$, with concretization $\gamma^\times$ as in definition 36.1.

Define $\alpha^\times \triangleq x \mapsto \prod_{i \in \Delta} \alpha_i(x)$ such that $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha^\times}{\overset{\gamma^\times}{\leftrightarrows}} \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$.

Let $\vec{\rho} \triangleq \vec{P} \mapsto \overrightarrow{\bigsqcap} \{ \vec{P}' \mid \gamma^\times(\vec{P}) \sqsubseteq \gamma^\times(\vec{P}') \}$ such that $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\vec{\rho} \circ \alpha^\times}{\overset{\gamma^\times}{\leftrightarrows}} \langle \vec{\rho}(\mathbb{P}^\times), \sqsubseteq^\times \rangle$.

Then $\vec{\rho}$ is meaning-preserving and $\langle \vec{\rho}(\mathbb{P}^\times), \sqsubseteq^\times \rangle$ is the reduced product of the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$, $i \in \Delta$.

This concludes our

- formal definition of the reduced product

from chapter 36, "Reduced Product"

The End

Principles of Abstract Interpretation

MIT press

Ch. 36, Reduced Product

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-36--reduced-product-PrAbsInt.pdf

Chapter 36

Ch. 36, Reduced Product (3/5)

In this third video, we study

- the iterated pairwise reduction

Iterated pairwise reduction, section 36.4

section 36.4.1, Pairwise reduction I

- The strong reduction operators ρ_γ of theorem 36.19 and $\vec{\rho}$ of theorem 36.24 involve all abstract domains of the direct product.
- They may be difficult to compute algorithmically.
- When adding a new abstract domain to increase precision of the analysis, the strong reduction between all domains must be completely redesigned.
- For simplicity, weaker reductions are useful.
- Pairwise reduction is an example of such a weak meaning-preserving of the direct product reduction.
- It applies between two abstract domains only and leaves the other domains unchanged.
- When a new abstract domain is added to the product of abstract domains of an abstract interpreter, one need only to design a pairwise reductions between the new abstract domain and (some of) the existing ones.
- Several weak reductions can be strengthen by iteration.

section 36.4.1, Pairwise reduction II

- This provides a general algorithm for constructing/approximating reduced products by iterated pairwise reductions, which can be implemented once for all in the static analyzer/verifier.

Definition (36.25, Pairwise reduction) Let $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$ be abstract domains with increasing concretization $\gamma_i \in \overline{\mathbb{P}}_i \xrightarrow{\nearrow} \mathbb{P}$ into the concrete domain $\langle \mathbb{P}, \sqsubseteq, \sqcap \rangle$.

Define $\gamma^\times(\vec{P}) \triangleq \bigwedge_{i \in \Delta} \gamma_i(\vec{P}_i)$ (as in definition 36.1).

For $i, j \in \Delta, i \neq j$, let $\rho_{ij} \in \langle \overline{\mathbb{P}}_i \times \overline{\mathbb{P}}_j, \sqsubseteq_{ij} \rangle \mapsto \langle \overline{\mathbb{P}}_i \times \overline{\mathbb{P}}_j, \sqsubseteq_{ij} \rangle$ be pairwise meaning-preserving reductions (so that $\forall \langle x, y \rangle \in \overline{\mathbb{P}}_i \times \overline{\mathbb{P}}_j \,.\, \rho_{ij}(\langle x, y \rangle) \sqsubseteq_{ij} \langle x, y \rangle$ and $(\gamma_i \times \gamma_j) \circ \rho_{ij} = (\gamma_i \times \gamma_j)$ [a]).

Define the pairwise reductions $\vec{\rho}_{ij} \in \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle \mapsto \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$ of the direct product as

$$\vec{\rho}_{ij}(\vec{P}) \quad \triangleq \quad \text{let } \langle \vec{P}'_i, \vec{P}'_j \rangle \triangleq \rho_{ij}(\langle \vec{P}_i, \vec{P}_j \rangle) \text{ in } \vec{P}[i \leftarrow \vec{P}'_i][j \leftarrow \vec{P}'_j]$$

where $\vec{P}[i \leftarrow x]_i = x$ and $\vec{P}[i \leftarrow x]_j = \vec{P}_j$ when $i \neq j$.

a. We define $(f \times g)(\langle x, y \rangle) \triangleq \langle f(x), g(y) \rangle$.

As shown in example 36.18, the reduction can be useful in a single domain to put abstract properties in so-called normal or canonical form.

Definition (36.27, Composition of pairwise reductions) Define the composition $\vec{\rho}$ of pairwise reductions $\{\vec{\rho}_{ij} \mid i, j \in \Delta\}$ of the direct product as

$$\vec{\rho} \triangleq \bigcirc_{i,j \in \Delta} \vec{\rho}_{ij} \tag{36.28}$$

where $\bigcirc_{i=1}^{n} f_i \triangleq f_{\pi_1} \circ \ldots \circ f_{\pi_n}$ is the function composition for some arbitrary permutation π of $[1, n]$.

Observe that $\vec{\rho}$ is the composition of finitely many meaning-preserving reductions so, by lemma 36.21, it is itself a meaning-preserving reduction.

section 36.4.2, Finitely iterated weak reduction

The precision of weak reductions during a a static analysis can be improved in the abstract by iteration without altering its soundness. This yields a weaker form of reduced product by iteration of weak reductions.

Definition (36.29, Iterated Reduction) Let the poset $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ be an abstract domain with concretization $\gamma \in \overline{\mathbb{P}} \rightarrowtail \mathbb{P}$ where $\langle \mathbb{P}, \sqsubseteq \rangle$ is the concrete domain and $\vec{\rho} \in \overline{\mathbb{P}} \to \overline{\mathbb{P}}$ be a meaning-preserving reduction ($\gamma \circ \vec{\rho} = \gamma$ and $\vec{\rho} \mathrel{\dot{\overline{\sqsubseteq}}} \mathbb{1}_{\overline{\mathbb{P}}}$).

The *finite iterates* of the reduction are $\vec{\rho}^{\,0} \triangleq \overline{P} \mapsto \overline{P}$, $\vec{\rho}^{\,n+1} = \vec{\rho} \circ \vec{\rho}^{\,n}$ for $n \in \mathbb{N}$.

Theorem (36.30, Finite iterated reduction) The finite iterates $\vec{\rho}^{\,n}, n \in \mathbb{N}$ of a meaning-preserving reduction $\vec{\rho}$ on $\langle \mathbb{P}, \overline{\sqsubseteq} \rangle$ are more precise in the abstract (since $\forall \vec{P} \in \mathbb{P}^{\times} \,.\, \forall n \in \mathbb{N}^{+} \,.\, \vec{\rho}^{\,n}(\vec{P}) \sqsubseteq^{\otimes} \vec{\rho}(\vec{P}) \sqsubseteq^{\otimes} \vec{\rho}_{ij}(\vec{P}) \sqsubseteq^{\otimes} \vec{P}, i, j \in \Delta$) and meaning-preserving (since $\vec{\rho}^{\,n}(\vec{P}), \vec{\rho}(\vec{P}), \vec{\rho}_{ij}(\vec{P}), \vec{P} \in [\vec{P}]_{\equiv^{\otimes}}$).

section 36.4.3, Iterated weak reduction is less precise than the reduced product

- The following examples prove that the iterated reduction may not be as precise as the reduced product.
- It is nevertheless easier to implement.

36.31, Iterated pairwise reduction of the direct product is not minimal

- Let us consider $\mathbb{P} = \wp(\{a, b, c\})$, $\overline{\mathbb{P}}_1 = \{\varnothing, \{a\}, \top\}$, $\overline{\mathbb{P}}_2 = \{\varnothing, \{a, b\}, \top\}$, $\overline{\mathbb{P}}_3 = \{\varnothing, \{a, c\}, \top\}$, and $\vec{P} = \langle \top,\ \{a, b\},\ \{a, c\} \rangle$ where $\top = \{a, b, c\}$.
- We have $\langle \top,\ \{a, b\},\ \{a, c\} \rangle / _{\equiv^{\otimes}} = \langle \{a\},\ \{a, b\},\ \{a, c\} \rangle$.
- However $\vec{\rho}_{ij}^{\rightarrow}(\langle \top,\ \{a, b\},\ \{a, c\} \rangle) = \langle \top,\ \{a, b\},\ \{a, c\} \rangle$ for $\Delta = \{1, 2, 3\}$, $i, j \in \Delta, i \neq j$ and so $\vec{\rho}^{\,*}(\langle \top,\ \{a, b\},\ \{a, c\} \rangle) = \langle \top,\ \{a, b\},\ \{a, c\} \rangle$
- proving, for that example, that $\vec{\rho}^{\,\star}(\langle \top,\ \{a, b\},\ \{a, c\} \rangle)$ is not a minimal element of $[\langle \top,\ \{a, b\},\ \{a, c\} \rangle]_{\equiv^{\otimes}}$.

example 36.32, Nelson-Oppen algorithm

- The satisfiability modulo theories (SMT) problem is a decision problem for logical formulas with respect to combinations of background theories expressed in classical first-order logic with equality.
- The Nelson-Oppen algorithm [Nelson and Oppen, 1979] combines decision procedures for these background theories. It is an iterated pairwise reduction [P. Cousot, R. Cousot, and Mauborgne, 2012].
- The reduction consists in propagating the equalities and inequalities between variables derived from one theory to all other theories.
- This is incomplete.
- For example assume that a theory of signs derives $x \geqslant 0$ and a theory of parity deriving that x is odd. None derives $x \neq 0$ because this is not an inequality between variables. So $x \geqslant 0$ is not reduced to $x > 0$.
- Completeness can be obtained by putting restrictions on the background theories, for example that they do not share symbols. So we cannot have both sign and parity background theories that share $+$, $-$, etc.

This concludes our study of

- the iterated pairwise reduction

from chapter 36, "Reduced Product"

The End

Principles of Abstract Interpretation

MIT press

Ch. 36, Reduced Product

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-36--reduced-product-PrAbsInt.pdf

Chapter 36

Ch. 36, Reduced Product (4/5)

In this fourth video, we study

- the (reduced) product transformers

(Reduced) product transformers, section 36.4.4

section 36.4.4, (Reduced) product transformers

The forward transformers $\mathsf{assign}_{\vec{\rho}}[\![\mathsf{x}, \mathsf{A}]\!]$ (19.12) are

$$\begin{array}{lcll} \mathsf{assign}_{\vec{r}}[\![\mathsf{x}, \mathsf{A}]\!]\ P & \triangleq & \mathsf{post}[\{\langle \rho,\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}]P & \\ & = & \{\rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho] \mid \rho \in P\} & (19.12) \\ \mathsf{assign}_{\vec{\mathsf{R}}}[\![\mathsf{x}, \mathsf{A}]\!]\ P & \triangleq & \mathsf{post}[\{\langle\langle \rho_0,\ \rho\rangle,\ \langle \rho_0,\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle\rangle \mid \rho_0, \rho \in \mathbb{E}\mathbb{v}\}]P & \\ & = & \{\langle \rho_0,\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle \mid \langle \rho_0,\ \rho\rangle \in P\} & \end{array}$$

Their reduced product abstractions proceed componentwise and reduce the result. (It may also be useful to reduce the arguments if this is not already the case).

Lemma (36.33) Let us consider a reduced product $\langle (\prod_{i\in\Delta} \overline{\mathbb{P}}_i)\,/_{\equiv^\otimes}, \sqsubseteq^\otimes\rangle$ of abstract domains $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i\rangle, i \in \Delta$ with concretizations $\gamma_i \in \overline{\mathbb{P}}_i \xrightarrow{\nearrow} C$ and sound forward transformers $\mathsf{assign}_{\vec{\mathtt{a}}_i}[\![\mathtt{x},\mathtt{A}]\!]$ such that $\mathsf{assign}_{\vec{\varrho}}[\![\mathtt{x},\mathtt{A}]\!]\gamma_i(\overline{P}) \subseteq \gamma_i(\mathsf{assign}_{\vec{\mathtt{a}}_i}[\![\mathtt{x},\mathtt{A}]\!]\overline{P})$ where $\mathsf{assign}_{\vec{\varrho}}[\![\mathtt{x},\mathtt{A}]\!] \in C \xrightarrow{\nearrow} C$ is the increasing concrete forward transformer. Similarly for backward transformers.
The corresponding transformer of a property $\vec{P} \in \prod_{i\in\Delta} \overline{\mathbb{P}}_i$ in the product is the reduction $\left(\prod_{i\in\Delta} \mathsf{assign}_{\vec{\mathtt{a}}_i}[\![\mathtt{x},\mathtt{A}]\!](\vec{P}_i)\right)/_{\equiv^\otimes}$ of the componentwise transformation.
This is sound since $\mathsf{assign}_{\vec{\varrho}}[\![\mathtt{x},\mathtt{A}]\!](\gamma^\otimes(\vec{P})) \subseteq \gamma^\otimes\left(\left(\prod_{i\in\Delta} \mathsf{assign}_{\vec{\mathtt{a}}_i}[\![\mathtt{x},\mathtt{A}]\!](\vec{P}_i)\right)/_{\equiv^\otimes}\right)$ and similarly for other transformers.

Proof of lemma 36.33

$$
\begin{aligned}
& \gamma^{\otimes}\left(\left(\prod_{i\in\Delta}\mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x},\mathsf{A}]\!](\vec{P}_i)\right)/_{\equiv^{\otimes}}\right) \\
= \quad & \gamma^{\otimes}\left(\prod_{i\in\Delta}\mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x},\mathsf{A}]\!](\vec{P}_i)\right) && \text{⟅def. reduced product⟆} \\
= \quad & \bigcap_{i\in\Delta}\gamma_i(\mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x},\mathsf{A}]\!](\vec{P}_i)) && \text{⟅def. } \gamma^{\otimes}\text{⟆} \\
\supseteq \quad & \bigcap_{i\in\Delta}\mathsf{assign}_{\vec{\varrho}}[\![\mathsf{x},\mathsf{A}]\!](\gamma_i(\vec{P}_i)) && \text{⟅soundness of the } \mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x},\mathsf{A}]\!]\text{⟆} \\
\supseteq \quad & \mathsf{assign}_{\vec{\varrho}}[\![\mathsf{x},\mathsf{A}]\!]\left(\bigcap_{i\in\Delta}\gamma_i(\vec{P}_i)\right) && \text{⟅assign}_{\vec{\varrho}}[\![\mathsf{x},\mathsf{A}]\!] \text{ increasing⟆} \\
= \quad & \mathsf{assign}_{\vec{\varrho}}[\![\mathsf{x},\mathsf{A}]\!](\gamma^{\otimes}(\vec{P})) && \text{⟅def. } \gamma^{\otimes}\text{.⟆} \quad \square
\end{aligned}
$$

- Unfortunately, this definition of the product transformer is not modular since it must be entirely redesigned when adding a new abstract domain to the product.
- Notice however, that abstract transformers themselves are elements of a reduced product, by defining their concretization as

Lemma (36.34) $\gamma^{\otimes}\left(\prod_{i\in\Delta} \mathsf{assign}_{\vec{\pi}_i}[\![\mathsf{x},\mathsf{A}]\!](\vec{P}_i)\right) = \vec{\gamma}\left(\prod_{i\in\Delta} \mathsf{assign}_{\vec{\pi}_i}[\![\mathsf{x},\mathsf{A}]\!]\right)(\vec{P})$.

Proof of lemma 36.34

$$
\begin{aligned}
& \gamma^{\otimes}\left(\prod_{i\in\Delta}\mathsf{assign}_{\vec{\mathfrak{A}}_i}\llbracket \mathsf{x},\mathsf{A}\rrbracket(\vec{P}_i)\right) \\
= \quad & \bigcap_{i\in\Delta}\gamma_i(\mathsf{assign}_{\vec{\mathfrak{A}}_i}\llbracket \mathsf{x},\mathsf{A}\rrbracket(\vec{P}_i)) && \text{⟅def. } \gamma^{\otimes}\text{⟆} \\
= \quad & \bigcap_{i\in\Delta}\dot{\gamma}_i(\mathsf{assign}_{\vec{\mathfrak{A}}_i}\llbracket \mathsf{x},\mathsf{A}\rrbracket)(\vec{P}) && \text{⟅pointwise definition } \dot{\gamma}_i(f)(\vec{x}) \triangleq \gamma_i(f(\vec{x}_i))\text{⟆} \\
= \quad & \left(\dot{\bigcap_{i\in\Delta}}\dot{\gamma}_i(\mathsf{assign}_{\vec{\mathfrak{A}}_i}\llbracket \mathsf{x},\mathsf{A}\rrbracket)\right)(\vec{P}) && \text{⟅pointwise def. } \left(\dot{\bigcap_{i\in\Delta}} f_i\right)(x) \triangleq \bigcap_{i\in\Delta} f_i(x)\text{⟆} \\
= \quad & \vec{\gamma}\left(\prod_{i\in\Delta}\mathsf{assign}_{\vec{\mathfrak{A}}_i}\llbracket \mathsf{x},\mathsf{A}\rrbracket\right)(\vec{P}) && \text{⟅def. } \vec{\gamma}(\prod_{i\in\Delta} f_i) \triangleq \dot{\bigcap_{i\in\Delta}}\dot{\gamma}_i(f_i)) \text{ for products.⟆} \quad \square
\end{aligned}
$$

- A direct consequence is that we can approximate the product transformer by iterated reduction of the componentwise transformers.

Backward transformers

- Define the backward transformers

$$\begin{array}{rcll} \mathsf{assign}^{\sim}_{\mathsf{T}}[\![\mathsf{x}, \mathsf{A}]\!]\, Q & \triangleq & \widetilde{\mathsf{pre}}[\{\langle \rho,\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}]Q & \\ & = & \{\rho \mid \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho] \in Q\} & (50.10) \\ \mathsf{assign}^{\sim}_{\mathsf{R}}[\![\mathsf{x}, \mathsf{A}]\!]\, Q & \triangleq & \widetilde{\mathsf{pre}}[\{\langle\langle \rho_0,\ \rho\rangle,\ \langle \rho_0,\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle\rangle \mid \rho_0, \rho \in \mathbb{E}\mathbb{v}\}] & \\ & = & \{\langle \rho_0,\ \rho\rangle \mid \langle \rho_0,\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle \in Q\} & \end{array}$$

- Observe that, by (12.22), we have the following Galois connection

Lemma (36.36) $\mathsf{assign}_{\vec{\wp}}[\![\mathsf{x}, \mathsf{A}]\!]\, P \subseteq Q \Leftrightarrow P \subseteq \mathsf{assign}_{\vec{\wp}}[\![\mathsf{x}, \mathsf{A}]\!]\, Q$.

iterated local reductions I

- It follows that if $\mathsf{assign}_{\vec{\wp}}[\![\mathsf{x}, \mathsf{A}]\!]\ P \subseteq Q$ then $\mathsf{assign}_{\vec{\wp}}[\![\mathsf{x}, \mathsf{A}]\!]\ (\mathsf{assign}_{\vec{\wp}}[\![\mathsf{x}, \mathsf{A}]\!]\ Q)$ is a more precise, sound over approximation of $\mathsf{assign}_{\vec{\wp}}[\![\mathsf{x}, \mathsf{A}]\!]\ P$ than Q, which suggests the following pairwise reduction $\dot{\rho}_{ij}$ of transformers (based on the pairwise reduction ρ_{ij} of abstract properties)

$$\begin{array}{l}
\dot{\rho}_{ij}(\langle \mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x}, \mathsf{A}]\!],\ \mathsf{assign}_{\dot{\mathfrak{A}}_j}[\![\mathsf{x}, \mathsf{A}]\!]\rangle) \quad \triangleq \\
\quad \langle x,\ y\rangle \mapsto \mathsf{let}\ \langle x',\ y'\rangle \triangleq \rho_{ij}(\langle \mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x}, \mathsf{A}]\!](x),\ \mathsf{assign}_{\dot{\mathfrak{A}}_j}[\![\mathsf{x}, \mathsf{A}]\!]\rangle(y))\ \mathsf{in} \\
\quad\quad \mathsf{let}\ \langle \grave{x},\ \grave{y}\rangle \triangleq \rho_{ij}(\langle x' \sqcap_i \mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x}, \mathsf{A}]\!](x),\ y' \sqcap_j \mathsf{assign}_{\dot{\mathfrak{A}}_j}[\![\mathsf{x}, \mathsf{A}]\!](y)\rangle)\ \mathsf{in} \\
\quad\quad\quad \rho_{ij}(\langle \mathsf{assign}_{\dot{\mathfrak{A}}_i}[\![\mathsf{x}, \mathsf{A}]\!](\grave{x}),\ \mathsf{assign}_{\dot{\mathfrak{A}}_j}[\![\mathsf{x}, \mathsf{A}]\!](\grave{y})\rangle)
\end{array}$$

which defines a reduction $\dot{\vec{\rho}}$ of transformers by (36.28) lifting the reduction $\vec{\rho}$ to the product of higher-order abstract properties.

Example: product of equality and sign analysis

- The componentwise forward propagation of $\langle a = b,\ \top \rangle$ through the assignment $a := \sqrt{b} + a$ is $\langle \top,\ b \geqslant 0 \rangle$ (with runtime error when $b < 0$ in which case execution is assumed to stop).
- The backward propagation yields the precondition $\langle a = b,\ b \geqslant 0 \rangle$ reduced to $\langle a = b,\ b \geqslant 0 \wedge a \geqslant 0 \rangle$
- The forward propagation is now reduced to $\langle \top,\ a \geqslant 0 \wedge b \geqslant 0 \rangle$.
- So the reduced componentwise forward propagation of $\langle a = b,\ \top \rangle$ through the assignment $a := \sqrt{b} + a$ is $\langle \top,\ a \geqslant 0 \wedge b \geqslant 0 \rangle$, which is more precise than $\langle \top,\ b \geqslant 0 \rangle$.

Example

An iterated reduction of the product of linear equalities and sign analyses of $\text{test}^{\vec{\partial}}[\![(x = y) \wedge ((z + 1) = x) \wedge (y = z)]\!]$ with precondition $x = 0$ yields the postcondition $x = 0 \wedge y = 0 \wedge z < 0$ (See [P. Cousot, 1999, Sect. 13.9]).

section 36.4.5, Widening

- The widening/narrowing [P. Cousot and R. Cousot, 1977] of a reduced product is often defined componentwise using widenings/narrowings of the component abstract domains.
- This ensures convergence for the product.
- However, it must be proved that the reduction does not break down the termination of the product widening, in which case reduction must be weakened or the widening strengthened [Cortesi and Zanioli, 2011].

Example

The closure operation in the zone abstract domain of chapter 40 can be considered as a reduction between separate domains, each considering only a pair of variables: if one applies the classical widening operation on zones followed by closure (reduction), then termination is no longer ensured as shown in section $40.1.8$ (same for the octagon abstract domain, see [Miné, 2006, Fig. 25–26]).

Practical implementation of the iterated pairwise reduction I

- Abstract interpreters are often built incrementally, by successively adding new abstract domains and combining them with already existing ones by pairwise iterated reduction.
- In order to avoid modifying existing domains, one can introduce a common interface between abstract domains representing the information propagated between abstract domain by the reduction.
- For Nelson-Oppen algorithm example 36.32 this can be equalities and disequalities between variables.
- For the reduced product of sign and parity in exercise 36.4 this can be equalities and disequalities between a variable and a constant.
- By asking the question $x \neq 0$?, the sign abstract domain can improve $x \leqslant 0$ to $x < 0$, $x \geqslant 0$ to $x > 0$, $x = 0$ to $\bot$, etc.

Practical implementation of the iterated pairwise reduction II

- This question can be answered e.g. by the parity abstract domain (when the parity of the variable and the constant differ), the constant abstract domain (when the variable is equal to a different constant), etc.
- Finally, for cost saving, the reduction in Definitions 36.25, 36.27, 36.29 need not be iterated until reaching a fixpoint.
- It can be stopped at any time, or even only a number of the possible reductions may be performed, even in a given order [Blazy, Bühler, and Yakobowski, 2017; Cortesi, Le Charlier, and Van Hentenryck, 2000; P. Cousot, R. Cousot, Feret, Mauborgne, Miné, Monniaux, and Rival, 2006; Jourdan, Laporte, Blazy, Leroy, and Pichardie, 2015].

Conclusion

Conclusion I

- More properties of reduced products are studied in [P. Cousot, R. Cousot, and Mauborgne, 2011].
- The reduced product and its variants are essential to extend static analyzers by introducing new abstractions without having to redo the whole static analyzer [P. Cousot, R. Cousot, Feret, Mauborgne, Miné, Monniaux, and Rival, 2006].
- Some static analyzers with a monolithic design like INFER [Calcagno, Distefano, Dubreil, Gabi, Hooimeijer, Luca, O'Hearn, Papakonstantinou, Purbrick, and Rodriguez, 2015] and more generally type inference [P. Cousot, 1997] lack this capacity of being simply extensible.
- Other compositions of abstract domains have been proposed in [Amato, Maio, and Scozzari, 2015; Cortesi, Filé, Giacobazzi, Palamidessi, and Ranzato, 1997; P. Cousot and R. Cousot, 1979; Filé and Ranzato, 1999; Giacobazzi and Ranzato, 1999; Giacobazzi and Scozzari, 1997].

Bibliography I

exchange the titles of the books of Mark A. Armstrong and George S. Simmons.

Amato, Gianluca, Simone Di Nardo Di Maio, and Francesca Scozzari (2015). "Sum of Abstract Domains.". In *NFM*. Vol. 9058. Lecture Notes in Computer Science. Springer, pp. 35–49.

Blazy, Sandrine, David Bühler, and Boris Yakobowski (2017). "Structuring Abstract Interpreters Through State and Value Abstractions.". In *VMCAI*. Vol. 10145. Lecture Notes in Computer Science. Springer, pp. 112–130.

Calcagno, Cristiano, Dino Distefano, Jérémy Dubreil, Dominik Gabi, Pieter Hooimeijer, Martino Luca, Peter W. O'Hearn, Irene Papakonstantinou, Jim Purbrick, and Dulma Rodriguez (2015). "Moving Fast with Software Verification.". In *NFM*. Vol. 9058. Lecture Notes in Computer Science. Springer, pp. 3–11.

Cortesi, Agostino, Gilberto Filé, Roberto Giacobazzi, Catuscia Palamidessi, and Francesco Ranzato (1997). "Complementation in Abstract Interpretation.". *ACM Trans.Program.Lang.Syst.*. 19.1, pp. 7–47.

Bibliography II

Cortesi, Agostino, Baudouin Le Charlier, and Pascal Van Hentenryck (2000). "Combinations of abstract domains for logic programming: open product and generic pattern construction.". *Sci.Comput.Program.*. 38.1-3, pp. 27–71.

Cortesi, Agostino and Matteo Zanioli (2011). "Widening and narrowing operators for abstract interpretation.". *Computer Languages, Systems & Structures*. 37.1, pp. 24–42.

Cousot, Patrick (1997). "Types as Abstract Interpretations.". In *POPL*. ACM Press, pp. 316–331.

— (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 (1977). "Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints.". In *POPL*. ACM, pp. 238–252.

— (1979). "Systematic Design of Program Analysis Frameworks.". In *POPL*. ACM Press, pp. 269–282.

Bibliography III

Cousot, Patrick, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, David Monniaux, and Xavier Rival (2006). "Combination of Abstractions in the Astrée Static Analyzer.". In *ASIAN*. Vol. 4435. Lecture Notes in Computer Science. Springer, pp. 272–300.

Cousot, Patrick, Radhia Cousot, and Laurent Mauborgne (2011). "The Reduced Product of Abstract Domains and the Combination of Decision Procedures.". In *FOSSACS*. Vol. 6604. Lecture Notes in Computer Science. Springer, pp. 456–472.

— (2012). "Theories, solvers and static analysis by abstract interpretation.". *J.ACM*. 59.6, 31:1–31:56.

Filé, Gilberto and Francesco Ranzato (1999). "The Powerset Operator on Abstract Interpretations.". *Theor.Comput.Sci.*. 222.1-2, pp. 77–111.

Giacobazzi, Roberto and Francesco Ranzato (1999). "The Reduced Relative Power Operation on Abstract Domains.". *Theor.Comput.Sci.*. 216.1-2, pp. 159–211.

Bibliography IV

Giacobazzi, Roberto and Francesca Scozzari (1997). "Intuitionistic Implication in Abstract Interpretation.". In *APPIA-GULP-PRODE*. Pp. 33–44.

Jourdan, Jacques-Henri, Vincent Laporte, Sandrine Blazy, Xavier Leroy, and David Pichardie (2015). "A Formally-Verified C Static Analyzer.". In *POPL*. ACM, pp. 247–259.

Miné, Antoine (2006). "The octagon abstract domain.". *Higher-Order and Symbolic Computation*. 19.1, pp. 31–100.

Nelson, Greg and Derek C. Oppen (1979). "Simplification by Cooperating Decision Procedures.". *ACM Trans.Program.Lang.Syst.*. 1.2, pp. 245–257.

This concludes our study of

- the reduced product transformers
- the direct and reduced products

from chapter 36, "Reduced Product"

The End

Principles of Abstract Interpretation

MIT press

Ch. 36, Reduced Product

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-36--reduced-product-PrAbsInt.pdf

Chapter 36

Ch. 36, Reduced Product (5/5)

In this last video, we (optionally) study

- the proofs of the reduced product theorems

Proofs

Definition (36.7, Reduced product (I)) Let $\mathbb{D} \triangleq \langle \mathbb{P}, \sqsubseteq, \bot, \sqcap, \sqcup, \mathsf{assign}[\![\mathsf{x},\mathsf{A}]\!], \mathsf{test}[\![\mathsf{B}]\!], \overline{\mathsf{test}}[\![\mathsf{B}]\!] \rangle$ be a concrete domain. Let $\overline{\mathbb{D}}^i \triangleq \langle \overline{\mathbb{P}}^i, \sqsubseteq^i, \bot^i, \sqcup^i, \mathsf{assign}_i[\![\mathsf{x},\mathsf{A}]\!], \mathsf{test}^i[\![\mathsf{B}]\!], \overline{\mathsf{test}}^i[\![\mathsf{B}]\!] \rangle$, $i \in \Delta$, Δ finite, be abstract domains with increasing concretization $\gamma_i \in \overline{\mathbb{P}}_i \xrightarrow{\nearrow} \mathbb{P}$. Let $\mathbb{D}^\times = \bigtimes_{i\in\Delta} \overline{\mathbb{D}}^i$ be their direct product with concretization $\gamma^\times$.

Their *reduced product* is $\mathbb{D}^\otimes \triangleq \bigotimes_{i\in\Delta} \overline{\mathbb{D}}^i \triangleq \langle \mathbb{P}^\otimes, \sqsubseteq^\otimes, \bot^\otimes, \sqcup^\otimes, \mathsf{assign}_\otimes[\![\mathsf{x},\mathsf{A}]\!], \mathsf{test}^\otimes[\![\mathsf{B}]\!], \overline{\mathsf{test}}^\otimes[\![\mathsf{B}]\!] \rangle$ where the reduced properties $\mathbb{P}^\otimes \triangleq \mathbb{P}^\times/_{\equiv^\otimes}$ are the equivalence classes of the equivalence relation $(\vec{P} \equiv^\otimes \vec{Q}) \triangleq (\gamma^\times(\vec{P}) = \gamma^\times(\vec{Q}))$ on the direct product $\mathbb{P}^\times$ and all operations are extended to these equivalence classes $\mathbb{P}^\otimes = \{[\vec{P}]_{\equiv^\otimes} \mid \vec{P} \in \mathbb{P}^\times\}$ of $\equiv^\otimes$ as follows.

- $\forall \vec{P} \in \mathbb{P}^\times \,.\, \gamma^\otimes([\vec{P}]_{\equiv^\otimes}) = \gamma^\times(\vec{P})$;
- $[\vec{P}]_{\equiv^\otimes} \sqsubseteq^\times [\vec{Q}]_{\equiv^\otimes} \triangleq \exists \vec{P}' \in [\vec{P}]_{\equiv^\otimes} \,.\, \exists \vec{Q}' \in [\vec{Q}]_{\equiv^\otimes} \,.\, \vec{P}' \sqsubseteq^\times \vec{Q}'$;
- $\bot^\otimes \triangleq [\bot]_{\equiv^\otimes}$;
- $\bigsqcup_{k\in K}^\otimes [\vec{P}_k]_{\equiv^\otimes} \triangleq [\bigsqcup_{k\in K}^\times \vec{P}_k]_{\equiv^\otimes}$;
- $\mathsf{assign}_\otimes[\![\mathsf{x},\mathsf{A}]\!][\vec{P}]_{\equiv^\otimes} \triangleq [\mathsf{assign}_\times[\![\mathsf{x},\mathsf{A}]\!]\vec{P}]_{\equiv^\otimes}$;
- $\mathsf{test}^\otimes[\![\mathsf{B}]\!][\vec{P}]_{\equiv^\otimes} \triangleq [\mathsf{test}^\times[\![\mathsf{B}]\!]\vec{P}]_{\equiv^\otimes}$;
- $\overline{\mathsf{test}}^\otimes[\![\mathsf{B}]\!][\vec{P}]_{\equiv^\otimes} \triangleq [\overline{\mathsf{test}}^\times[\![\mathsf{B}]\!]\vec{P}]_{\equiv^\otimes}$.

Reminder

- more precise

$$\overline{\mathbb{P}}_1 \mathrel{\widehat{\leqslant}} \overline{\mathbb{P}}_2 \quad \triangleq \quad \gamma_2(\overline{\mathbb{P}}_2) \subseteq \gamma_1(\overline{\mathbb{P}}_1)$$

- $\langle \mathbb{P}, \sqsubseteq, \sqcap \rangle$ is closed by intersection

$$\forall P, Q \in \mathbb{P} \,.\, \exists R \in \mathbb{P} \,.\, \gamma(R) = \gamma(P) \sqcap \gamma(Q)$$

Theorem (36.14, Equivalent definition of the reduced product (II)) Let the meet semi-lattice $\langle \mathbb{P}, \sqsubseteq, \top, \sqcap \rangle$ be concrete properties;
Let $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i, \top_i \rangle$, $i \in \Delta$, Δ finite, be abstract properties with increasing concretization $\gamma_i \in \overline{\mathbb{P}}_i \xrightarrow{\nearrow} \mathbb{P}$ and supremum $\top_i$ such that $\gamma_i(\top_i) = \top$.

The reduced product $\langle \mathbb{P}^\times/_{\equiv^\otimes}, \sqsubseteq^\otimes, [\vec{\top}]_{\equiv^\otimes} \rangle$ is the greatest lower bound of the $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i \rangle$, $i \in \Delta$ in that it is

- more precise than $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$, $i \in \Delta$,
- less precise than any other $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$, which is closed by finite intersection and more precise than all the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$, $i \in \Delta$.

If $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i, \top_i \rangle$, $i \in \Delta$ are closed by finite intersection then their reduced product $\langle \mathbb{P}^\times/_{\equiv^\otimes}, \sqsubseteq^\otimes, [\vec{\top}]_{\equiv^\otimes} \rangle$ is the unique such domain of abstract properties (up to the equivalence $\hat{\equiv}$).

Proof of theorem 36.14 — For all $i \in \Delta$ and $P_i \in \overline{\mathbb{P}}_i$, we have
$\gamma^{\otimes}([\overrightarrow{\top}]_{\equiv^{\otimes}}[i \leftarrow P_i]) \triangleq \bigsqcap_{j \in \Delta \setminus \{i\}} \gamma_i(\top_j) \sqcap \gamma_i(P_i) = \bigsqcap_{j \in \Delta \setminus \{i\}} \top \sqcap \gamma_i(P_i) = \top \sqcap \gamma_i(P_i) = \gamma_i(P_i)$
proving that $\gamma_i(\overline{\mathbb{P}}_i) \subseteq \gamma^{\otimes}(\mathbb{P}^{\times}/_{\equiv^{\otimes}})$
so that $\langle \mathbb{P}^{\times}/_{\equiv^{\otimes}}, \sqsubseteq^{\otimes} \rangle$ is more precise than the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle, i \in \Delta$.

— If $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ with $\overline{\gamma} \in \overline{\mathbb{P}} \rightleftarrows \mathbb{P}$ is more precise than the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$ then $\gamma_i(\overline{\mathbb{P}}_i) \subseteq \overline{\gamma}(\overline{\mathbb{P}})$.
Given $\overrightarrow{P} \in \mathbb{P}^{\times}/_{\equiv^{\otimes}}$, $\exists \overline{P}_i \,.\, \overline{\gamma}(\overline{P}_i) = \gamma_i(\overrightarrow{P}_i)$ so $\exists \overline{P} \in \overline{\mathbb{P}} \,.\, \overline{\gamma}(\overline{P}) = \bigsqcap_{i \in \Delta} \overline{\gamma}(\overline{P}_i) = \bigsqcap_{i \in \Delta} \gamma_i(\overrightarrow{P}_i) \triangleq \gamma^{\otimes}(\overrightarrow{P})$ since $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ is closed by finite intersection and Δ is finite.
It follows that $\gamma^{\otimes}(\mathbb{P}^{\times}/_{\equiv^{\otimes}}) \subseteq \overline{\gamma}(\overline{\mathbb{P}})$.

— The property is characteristic since the $\langle \overline{\mathbb{P}}_i, \sqsubseteq_i, \top_i \rangle, i \in \Delta$ are closed by finite intersection so that their reduced product $\langle \mathbb{P}^{\times}/_{\equiv^{\otimes}}, \sqsubseteq^{\otimes}, [\overrightarrow{\top}]_{\equiv^{\otimes}} \rangle$ is also closed by intersection and therefore any other abstract domain $\langle \overline{\overline{\mathbb{P}}}, \overline{\overline{\sqsubseteq}} \rangle$ with the same property would have both $\gamma^{\otimes}(\mathbb{P}^{\times}/_{\equiv^{\otimes}}) \subseteq \overline{\overline{\gamma}}(\overline{\overline{\mathbb{P}}})$ and $\overline{\overline{\gamma}}(\overline{\overline{\mathbb{P}}}) \subseteq \gamma^{\otimes}(\mathbb{P}^{\times}/_{\equiv^{\otimes}})$ hence would, by antisymmetry, be an equivalent domain of abstract properties. □

Theorem (36.19, Reduction Operator) Let $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ where $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq}, \overline{\bot}, \overline{\top}, \overline{\sqcup}, \overline{\sqcap} \rangle$ is a complete lattice. Define

$$\rho_\gamma(a) \triangleq \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a')\}$$

then ρ_γ is a lower closure (reductive, increasing and idempotent) on $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ and

$$\langle \mathbb{P}, \sqsubseteq \rangle \underset{\rho_\gamma \circ \alpha}{\overset{\gamma}{\leftrightarrows}} \langle \rho_\gamma(\overline{\mathbb{P}}), \overline{\sqsubseteq} \rangle .$$

Proof of theorem 36.19 —— ρ_γ is reductive since $a \in \{a' \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a')\}$ by reflexivity and so $\rho_\gamma(a) \sqsubseteq a$ by def. glb $\sqcap$.

—— If $a \sqsubseteq b$ then $\gamma(a) \sqsubseteq \gamma(b)$ so $\gamma(b) \sqsubseteq \gamma(b')$ implies $\gamma(a) \sqsubseteq \gamma(b')$ hence $\{b' \mid \gamma(b) \sqsubseteq \gamma(b')\} \subseteq \{a' \mid \gamma(a) \sqsubseteq \gamma(a')\}$ so $\rho_\gamma(a) = \overline{\bigsqcap}\{a' \mid \gamma(a) \sqsubseteq \gamma(a')\} \sqsubseteq \overline{\bigsqcap}\{b' \mid \gamma(b) \sqsubseteq \gamma(b')\} = \rho_\gamma(b)$.

—— For idempotence, we have

$$
\begin{aligned}
& \rho_\gamma(\rho_\gamma(a)) \\
= & \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(\rho_\gamma(a)) \sqsubseteq \gamma(a')\} && \text{(def. } \rho_\gamma\text{)} \\
= & \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(\overline{\bigsqcap}\{a'' \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a'')\}) \sqsubseteq \gamma(a')\} && \text{(def. } \rho_\gamma\text{)} \\
= & \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \bigsqcap\{\gamma(a'') \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a'')\} \sqsubseteq \gamma(a')\} \\
& && \text{(in a Galois connection, } \gamma \text{ preserves preserves existing glbs)} \\
= & \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a')\} \\
& && \text{(since } \gamma(a) = \bigsqcap\{\gamma(a'') \in \overline{\mathbb{P}} \mid \gamma(a) \sqsubseteq \gamma(a'')\} \text{ by reflexivity and def. glb)} \\
= & \rho_\gamma(a) && \text{(def. } \rho_\gamma\text{)}
\end{aligned}
$$

— We conclude that ρ_γ is a lower closure (reductive, increasing and idempotent) on $\overline{\mathbb{P}}$.

— If $x \in \mathbb{P}$ and $y \in \rho_\gamma(\overline{\mathbb{P}})$ then $y \in \overline{\mathbb{P}}$ so, by the Galois connection, $x \sqsubseteq \gamma(y)$ implies $\alpha(x) \sqsubseteq y$ implies $\rho_\gamma \circ \alpha(x) \sqsubseteq y$ since ρ_γ is reductive.

— Conversely, if $x \in \mathbb{P}$ and $y \in \rho_\gamma(\overline{\mathbb{P}})$ then

$$
\begin{array}{lll}
& \rho_\gamma \circ \alpha(x) \sqsubseteq y & \\
\Rightarrow & \overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(\alpha(x)) \sqsubseteq \gamma(a')\} \sqsubseteq y & \text{(def. } \circ \text{ and } \rho_\gamma\text{)} \\
\Rightarrow & \gamma(\overline{\bigsqcap}\{a' \in \overline{\mathbb{P}} \mid \gamma(\alpha(x)) \sqsubseteq \gamma(a')\}) \sqsubseteq \gamma(y) & \text{(in a Galois connection, } \gamma \text{ increasing)} \\
\Rightarrow & (\bigsqcap\{\gamma(a') \in \overline{\mathbb{P}} \mid \gamma(\alpha(x)) \sqsubseteq \gamma(a')\}) \sqsubseteq \gamma(y) & \\
& & \text{(in a Galois connection, } \gamma \text{ preserves existing glbs)} \\
\Rightarrow & \gamma \circ \alpha(x) \sqsubseteq \gamma(y) & \text{(reflexivity for } a' = \alpha(x) \text{ and def. glb)} \\
\Rightarrow & x \sqsubseteq \gamma(y) & \text{(in a Galois connection, } \gamma \circ \alpha \text{ is extensive and transitivity)}
\end{array}
$$

□

- $\rho \in \overline{\mathbb{P}} \to \overline{\mathbb{P}}$ is *meaning-preserving* iff $\forall \overline{P} \in \overline{\mathbb{P}} \,.\, \gamma(\rho(\overline{P})) = \gamma(\overline{P})$.

- The following theorem shows that the reduction ρ_γ is meaning-preserving that is does not change the expressiveness of the reduced abstract properties.

> **Theorem (36.22)** With the hypotheses of theorem 36.19, ρ_γ is meaning-preserving, $\gamma = \gamma \circ \rho_\gamma$.

Proof of theorem 36.22 For all $x \in \mathbb{P}$:

$$
\begin{aligned}
& \gamma \circ \rho_\gamma \circ \alpha(x) \\
= \; & \gamma(\overline{\bigsqcap}\{a \mid \gamma(\alpha(x)) \sqsubseteq \gamma(a)\}) && \text{⟅def. } \rho_\gamma \text{⟆} \\
= \; & \bigsqcap\{\gamma(a) \mid \gamma(\alpha(x)) \sqsubseteq \gamma(a)\}) && \text{⟅in a Galois connection, } \gamma \text{ preserves meets⟆} \\
= \; & \gamma(\alpha(x)) && \text{⟅choosing } a = \alpha(x) \text{ and def. glb⟆}
\end{aligned}
$$

and so

$$
\begin{aligned}
& \gamma \\
= \; & \gamma \circ \alpha \circ \gamma && \text{⟅Galois connection⟆} \\
= \; & \gamma \circ \rho_\gamma \circ \alpha \circ \gamma && \text{⟅since } \gamma \circ \alpha = \gamma \circ \rho_\gamma \circ \alpha \text{⟆} \\
\dot{\sqsubseteq} \; & \gamma \circ \rho_\gamma && \text{⟅} \alpha \circ \gamma \text{ is reductive and } \gamma \text{ and } \rho_\gamma \text{ are increasing⟆}
\end{aligned}
$$

Moreover ρ_γ is a lower closure on $\langle \overline{\mathbb{P}}, \overline{\sqsubseteq} \rangle$ so ρ_γ is reductive ($\rho_\gamma \mathrel{\dot{\overline{\sqsubseteq}}} \mathbb{1}$) hence $\gamma \circ \rho_\gamma \mathrel{\dot{\sqsubseteq}} \gamma$ since γ is increasing. By antisymmetry, $\gamma \circ \rho_\gamma = \gamma$. □

Theorem (36.24, Equivalent definition of the reduced product (III)) Let $\langle \mathbb{P}, \sqsubseteq \rangle$ be a poset; Let $\forall i \in \Delta, \Delta$ finite, each $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i, \overline{\bot}_i, \overline{\top}_i, \overline{\sqcup}_i, \overline{\sqcap}_i \rangle$ be a complete lattice such that $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_i}{\overset{\gamma_i}{\leftrightarrows}} \langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$.

Let $\langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$ be the direct product of the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle, i \in \Delta$, with concretization $\gamma^\times$ as in definition 36.1.

Define $\alpha^\times \triangleq x \mapsto \prod_{i \in \Delta} \alpha_i(x)$ such that $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha^\times}{\overset{\gamma^\times}{\leftrightarrows}} \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$.

Let $\vec{\rho} \triangleq \vec{P} \mapsto \overrightarrow{\bigsqcap} \{\vec{P}' \mid \gamma^\times(\vec{P}) \sqsubseteq \gamma^\times(\vec{P}')\}$ such that $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\vec{\rho} \circ \alpha^\times}{\overset{\gamma^\times}{\leftrightarrows}} \langle \vec{\rho}(\mathbb{P}^\times), \sqsubseteq^\times \rangle$.

Then $\vec{\rho}$ is meaning-preserving and $\langle \vec{\rho}(\mathbb{P}^\times), \sqsubseteq^\times \rangle$ is lattice-isomorphic to the reduced product of the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle, i \in \Delta$.

Proof of theorem 36.24 —— $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_\times}{\overset{\gamma_\times}{\leftrightarrows}} \langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$ and $\langle \mathbb{P}^\times, \sqsubseteq^\times \rangle$ is a complete lattice follow componentwise from the hypothesis $\forall i \in \Delta \,.\, \langle \mathbb{P}, \sqsubseteq \rangle \underset{\alpha_i}{\overset{\gamma_i}{\leftrightarrows}} \langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$ and $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle$ is a complete lattice.

—— $\vec{\rho}$ is defined as ρ_γ in theorem 36.19 so $\langle \mathbb{P}, \sqsubseteq \rangle \underset{\vec{\rho} \circ \alpha_\times}{\overset{\gamma_\times}{\leftrightarrows}} \langle \vec{\rho}(\mathbb{P}^\times), \sqsubseteq^\times \rangle$, $\vec{\rho}$ is a lower closure operator, and by theorem 36.22, it is meaning preserving.

—— By def. $(\vec{P} \equiv^\otimes \vec{Q}) \triangleq (\gamma^\times(\vec{P}) = \gamma^\times(\vec{Q}))$ in definition 36.7, if follows that $[\vec{P}]_{\equiv^\otimes} = [\vec{\rho}(\vec{P})]_{\equiv^\otimes}$ proving that $\langle \vec{\rho}(\mathbb{P}^\times), \sqsubseteq^\times \rangle$ is a complete lattice isomorphic to the reduced product $\langle \mathbb{P}^\otimes, \sqsubseteq^\otimes \rangle$ of the $\langle \overline{\mathbb{P}}_i, \overline{\sqsubseteq}_i \rangle, i \in \Delta$. □

Theorem (36.30, Finite iterated reduction) The finite iterates $\vec{\rho}^{\,n}, n \in \mathbb{N}$ of a meaning-preserving reduction $\vec{\rho}$ on $\langle \mathbb{P}, \overline{\sqsubseteq} \rangle$ are more precise in the abstract (since $\forall \vec{P} \in \mathbb{P}^{\times} \,.\, \forall n \in \mathbb{N}^{+} \,.\, \vec{\rho}^{\,n}(\vec{P}) \sqsubseteq^{\otimes} \vec{\rho}(\vec{P}) \sqsubseteq^{\otimes} \vec{\rho}_{ij}(\vec{P}) \sqsubseteq^{\otimes} \vec{P}, i, j \in \Delta$) and meaning-preserving (since $\vec{\rho}^{\,n}(\vec{P}), \vec{\rho}(\vec{P}), \vec{\rho}_{ij}(\vec{P}), \vec{P} \in [\vec{P}]_{\equiv^{\otimes}}$).

Proof of theorem 36.30 Let $\langle \rho^n, n \in \mathbb{N} \rangle$ be the iterates of a meaning-preserving reduction ρ.
Observe, by recurrence, that the iterates form a descending chain since ρ is reductive so $\forall n < m \,.\, \rho^n(\overline{P}) \sqsubseteq \rho^n(\overline{P}) \sqsubseteq \overline{P}$.
Meaning-preservation follows by recurrence.
For the basis, $\gamma(\rho^0(\overline{P})) = \gamma(\overline{P})$ by def. of ρ^0.
For induction, $\gamma(\rho^{n+1}(\overline{P})) \triangleq \gamma(\rho(\rho^n(\overline{P}))) = \gamma(\rho^n(\overline{P})) = \gamma(\overline{P})$, since ρ is meaning-preserving and by induction hypothesis. □

Home work

Read Ch. 36 “Reduced Product” of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you