Closed and logical relations for over- and under-approximation of powersets

David Schmidt

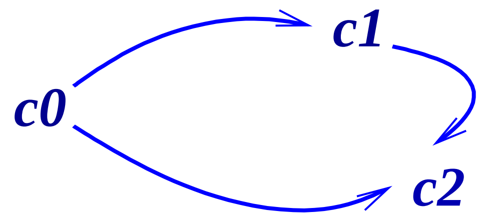
Kansas State University
and École Polytechnique

www.cis.ksu.edu/~schmidt

Motivation

Dennis Dams's *mixed transition systems*

$$\Sigma = \{c_0, c_1, c_2\}$$
$$R = \{(c_0, c_1), (c_0, c_2), (c_1, c_2)\}$$



Approximating the states: Note: $\bot$ and $\top$ omitted for brevity.

$$\alpha\{c_0\} = a_0, \qquad \alpha\{c_1\} = a_{12} = \alpha\{c_2\} = \alpha\{c_1, c_2\}$$

Over-approximation transitions ("*may*" : $\exists\exists$) for safety properties:

$$\alpha\Sigma = \{a_0, a_{12}\}$$
$$R^\sharp = \{(a_0, a_{12}), (a_{12}, a_{12})\}$$

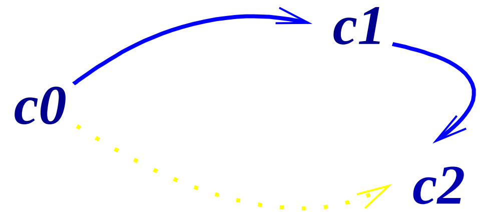
Under-approximation transitions ("*must*" : $\forall\exists$) for liveness properties:

$$\alpha\Sigma = \{a_0, a_{12}\}$$
$$R^\flat = \{(a_0, a_{12})\}$$

A *mixed transition system* is $(\alpha\Sigma, R^\flat, R^\sharp)$.

Note that the $\forall\exists$-definition of under-approximation is not the only candidate:

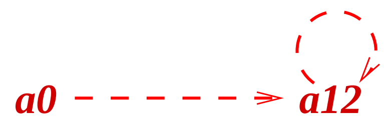
$$\Sigma = \{c_0, c_1, c_2\}$$
$$R = \{(c_0, c_1), (c_1, c_2)\}$$



State abstraction:

$$\alpha\{c_0\} = a_0, \qquad \alpha\{c_1\} = a_{12} = \alpha\{c_2\} = \alpha\{c_1, c_2\}$$

The $\exists\exists$-over-approximation remains the same:

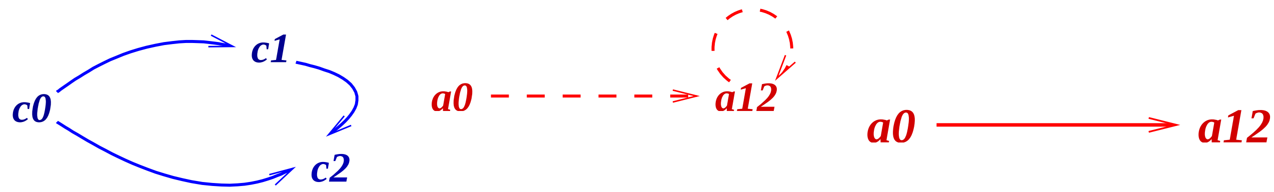


Under-approximation transitions ($\forall\exists$):

$$\alpha\Sigma = \{a_0, a_{12}\}$$
$$R^\flat = \{(a_0, a_{12})\}$$

Under-approximation transitions ($\forall\forall$):

$$\alpha\Sigma = \{a_0, a_{12}\}$$
$$R^\flat = \{\ \}$$



From Galois connection, $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$, Dams defines this *simulation relation*: $c\ \rho\ a$ *iff* $c \in \gamma(a)$. For $R \subseteq C \times C$, he defines

$$aR^{\sharp}a' \text{ iff } a' \in \{\alpha(Y) \mid Y \in \min\{S' \mid R^{\exists\exists}(\gamma(a), S')\}\}$$
$$aR^{\flat}a' \text{ iff } a' \in \{\alpha(Y) \mid Y \in \min\{S' \mid R^{\forall\exists}(\gamma(a), S')\}\}$$

and he proves $R \lhd_{\rho} R^{\sharp}$: $R^{\sharp}$ ρ-*simulates* R

$R^{\flat} \lhd_{\rho^{-1}} R$: $R^{\flat}$ *is* ρ-*simulated by* R

This gives him soundness for $\Box$ ($\forall R$) and $\Diamond$ ($\exists R$): *If*

$$a \models \Box\phi \textit{ iff for all } a', aR^{\sharp}a' \textit{ implies } a' \models \phi$$
$$a \models \Diamond\phi \textit{ iff there exists } a' \textit{ such that } aR^{\flat}a' \textit{ and } a' \models \phi$$

then, $a \models \phi$ *and* $c\ \rho\ a$ *imply* $c \models \phi$*.*

And with lots of hard work, he proves "best precision": Of all the ρ-, ρ^{-1}-simulations of R, $R^{\sharp}$ and $R^{\flat}$ preserve the *most* $\Box\Diamond$-properties.

Can we prove the over- and under-approximation results directly from Galois-connection theory?

Yes — we treat $R \subseteq C \times C$ as $R : C \to \mathcal{P}(C)$.
Then, $R^\sharp : A \to \mathcal{P}_L A$, where $\mathcal{P}_L$ is a *lower powerset* ($\sqsubseteq$) constructor.

We "lift" the Galois connection, $\mathcal{P}(C)\langle\alpha, \gamma\rangle A$, on the states to a higher-order Galois connection on transition relations:

$$C \to PC\langle\alpha', \gamma'\rangle A \to \mathcal{P}_L A$$

so that

1. $R \lhd_\rho R^\sharp$ *iff* $R \circ \gamma' \sqsubseteq \gamma' \circ R^\sharp$
2. *soundness of* $a \models \phi$ *follows from* 1.
3. $R^\sharp_{best} = \alpha' \circ R \circ \gamma$

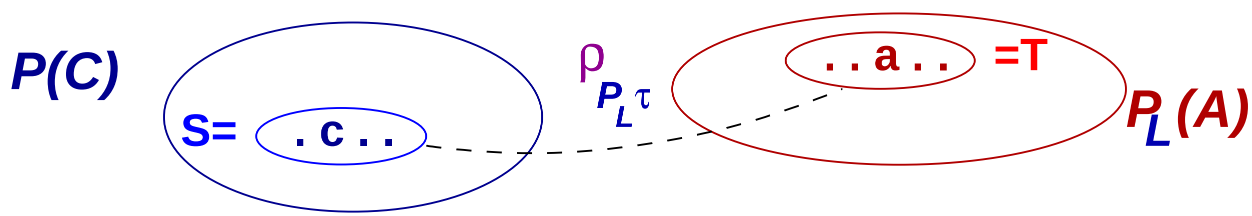
And we do similar but harder work for $R^\flat : A \to \mathcal{P}_U A$, where $\mathcal{P}_U$ is an *upper powerset* ($\sqsupseteq$) constructor.

And there are interesting choices for α', γ', PC, $\mathcal{P}_L$, *and* $\mathcal{P}_U$....

Let $R^\sharp : A \rightarrow \mathcal{P}_L A$.
How do we concretize a set $T \in \mathcal{P}_L A$?

Given Galois connection, $\mathcal{P}(C)\langle\alpha,\gamma\rangle A_\tau$, say $c\ \rho_\tau\ a$ *iff* $c \in \gamma(a)$: c *is approximated by* a .

Choice 1: let $S \in \mathcal{P}(C)$ and $T \in \mathcal{P}_L A$:



S is over-approximated by T iff for every $c \in S$, there exists some $a \in T$ such that c is approximated by a:

$$S\ \rho_{\mathcal{P}_L(\tau)}\ T \textit{ iff for every } c \in S, \textit{ there exists } a \in T \textit{ such that } c\ \rho_\tau\ a$$

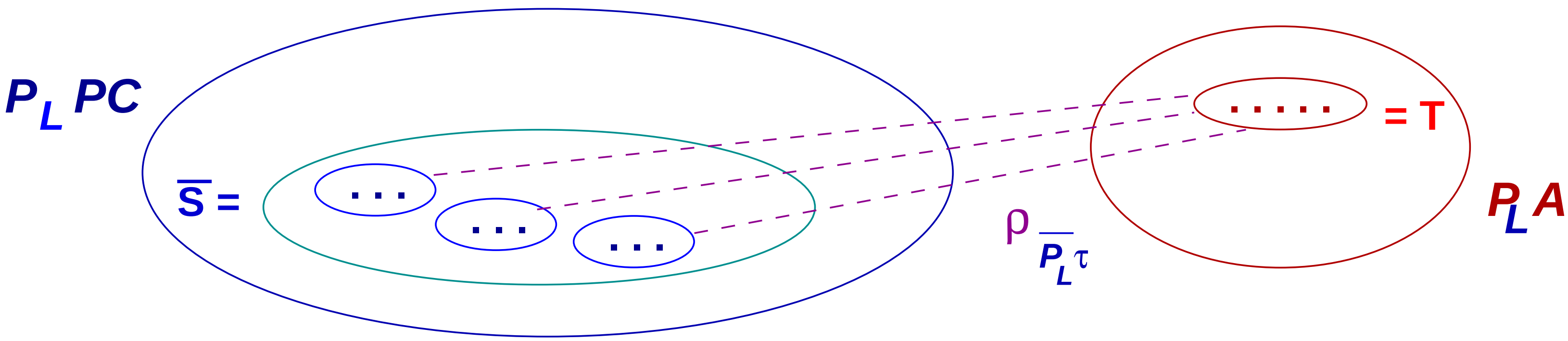
Then,

$$\gamma_{\mathcal{P}_L\tau}(T) = \cup\{S \mid S\ \rho_{\mathcal{P}_L\tau}\ T\} = \{c \mid \text{exists } a \in T, c\ \rho_\tau\ a\}$$

When $\rho_\tau \subseteq C \times C$ equals $\sqsubseteq_\tau$, then $\rho_{\mathcal{P}_L\tau}$ is half of the Egli-Milner ordering and freely generates the lower (“Hoare”) powerdomain.

Choice 2: The concrete domain might be $\mathcal{P}_L(\mathcal{P}(C))$: sets of sets of states. *Intuition:* if abstract state $a \in A_\tau$ concretizes to a *set of states*, $\gamma(a) \subseteq C$, then set $T \in \mathcal{P}_L A_\tau$ should concretize to a *set of sets*.

We have this relationship:



That is, $\bar{S} \in \mathcal{P}_L(\mathcal{P}(C))$ is over-approximated by $T \in \mathcal{P}_L A_\tau$ if for every set $S \in \bar{S}$, $S \, \rho_{\mathcal{P}_L(\tau)} \, T$.

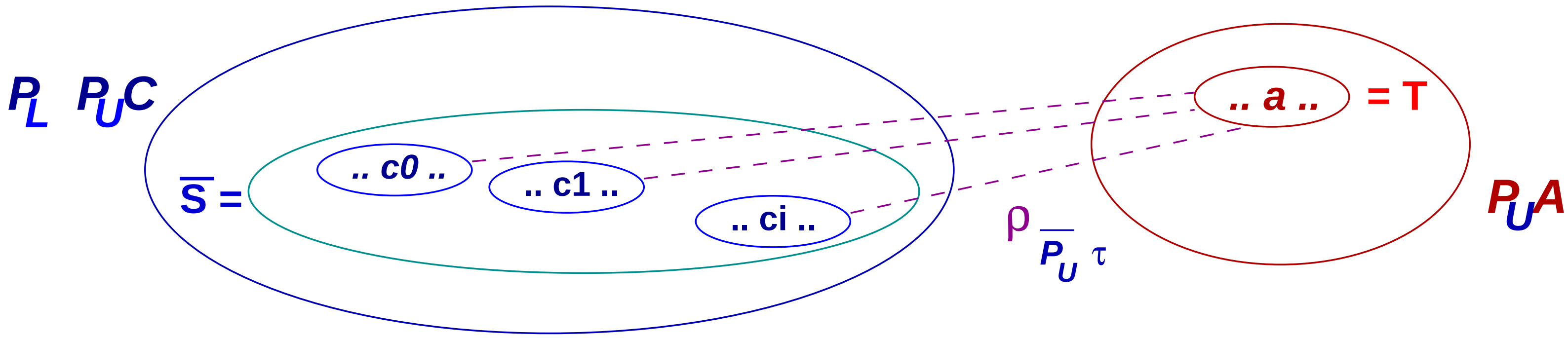
This makes

$$\gamma_{\bar{\mathcal{P}}_L \tau}(T) = \{S \mid S \, \rho_{\mathcal{P}_L \tau} \, T\}$$

This definition is the "same" as the one on the previous slide in the sense that $\bigcup \gamma_{\bar{\mathcal{P}}_L \tau}(T) = \gamma_{\mathcal{P}_L \tau}(T)$.

Either can be used to define a sound and best $R^\sharp : A \to \mathcal{P}_L A_\tau$.

But we define the under-approximation, $R^\flat : A \to \mathcal{P}_U A$ with Choice 2, mapping sets $T \in \mathcal{P}_U A$ to sets of sets in $\mathcal{P}_L(\mathcal{P}_U C)$:



That is, $\bar{S}$ is approximated by T iff *for every set $S \in \bar{S}$, S is under-approximated by T,* written as $S \, \rho_{\mathcal{P}_U(\tau)} \, T$, where

$S \, \rho_{\mathcal{P}_U(\tau)} \, T$ *iff for every $a \in T$, there exists some $c \in S$ such that $c \, \rho_\tau \, a$.*

This makes

$$\gamma_{\bar{\mathcal{P}}_U A_\tau}(T) = \{S \mid S \, \rho_{\mathcal{P}_U \tau} \, T\}$$

which has a different significance than $\gamma_{\mathcal{P}_U A_\tau}(T) = \bigcup \gamma_{\bar{\mathcal{P}}_U A_\tau}(T)$!

Choice 2 gives us a useful, sound $R^\flat : A \to \mathcal{P}_U A$.

When $\rho_\tau \subseteq C \times C$ is $\sqsubseteq_\tau$, then $\rho_{\mathcal{P}_U \tau}$ is the other half of the Egli-Milner ordering and freely generates the upper ("Smyth") powerdomain.

Example: Let Nat be the set of natural numbers and let complete lattice $\mathsf{Polarity} = \{\mathsf{none}, \mathsf{even}, \mathsf{odd}, \mathsf{any}\}$.

Define $\rho : \mathsf{Nat} \times \mathsf{Polarity}$ in the obvious way: $2\ \rho\ \mathsf{even}$, $2\ \rho\ \mathsf{any}$, $3\ \rho\ \mathsf{odd}$, etc.

We define a Galois connection on $\mathcal{P}(\mathsf{Nat})$ and $\mathsf{Polarity}$ and lift it:

$$\gamma : \mathcal{P}_{\uparrow}\mathsf{Polarity} \rightarrow \mathcal{P}_{\downarrow}(\mathcal{P}(\mathsf{Nat})^{op})$$

$\gamma\{\} =$ all subsets of nats

$\supseteq$

$\gamma\{\mathsf{any}\} =$ nonempty subsets of nats

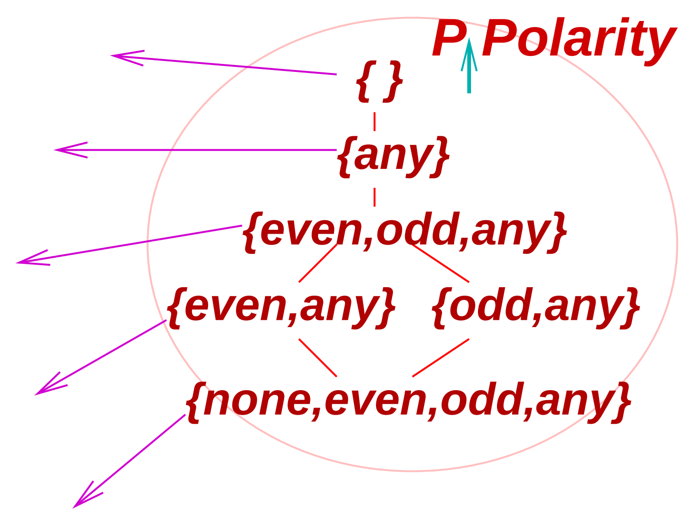
$\supseteq$

$\gamma\{\mathsf{even}, \mathsf{odd}, \mathsf{any}\} =$ all sets with 1+ even and 1+ odd $\supseteq$

$\gamma\{\mathsf{even}, \mathsf{any}\} =$ all sets with 1+ even

$\supseteq$

$\gamma \uparrow\mathsf{none} =$ empty set



Our results from reworking Dams's constructions

1. Starting from approximation relations, $\rho \subseteq C \times A$, we generate Galois connections from such U-GLB-L-LUB-closed relations cf. [*Mycroft-Jones 86, Cousot-Cousot JLC 92*].

2. We define lower and upper powerset constructions, weaker forms of powerdomain but strong enough for abstraction studies. The former are the *join completions* of [*Cousot-Cousot ICCL 94*].

3. We use the powerset types in a family of logical relations, show how the family preserves the closure properties in 1., and prove that a simulation proof is an instance of proof via logical relations. We obtain Dams's most-precise simulation results "for free." We compare to earlier attempts by [*Loiseaux, et al. 95, Backhouse-Backhouse 98*].

4. We extract validation and refutation logics from the logical relations, state their resemblance to Hennessy-Milner logic (and description logic), and obtain easy proofs of soundness.

Closed relations

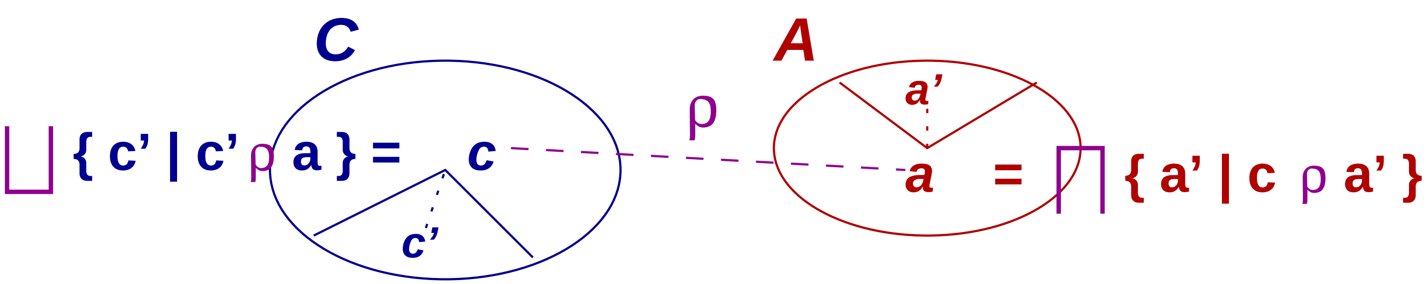
Closed relations and Galois connections

Let C and A be complete lattices, and let $\rho \subseteq C \times A$.

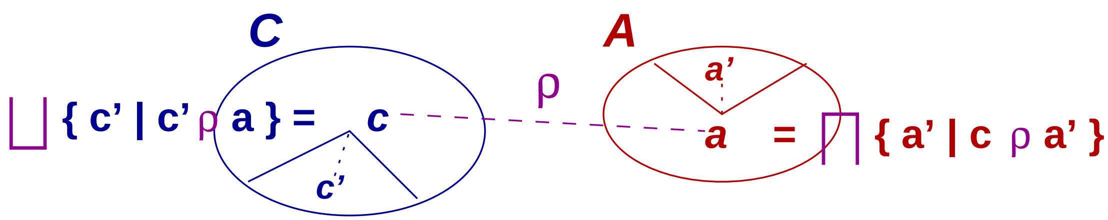
$c \; \rho \; a$ means that c is modelled/approximated by a

Definition: For all $c, c' \in C$, $a, a' \in A$, for $\rho \subseteq C \times A$, ρ is

1. *U-closed* iff $c \; \rho \; a$, $a \sqsubseteq a'$ imply $c \; \rho \; a'$
2. *GLB-closed* iff $c \; \rho \; \sqcap \{a \mid c \; \rho \; a\}$
3. *L-closed* iff $c \; \rho \; a$, $c' \sqsubseteq c$ imply $c' \; \rho \; a$
4. *LUB-closed* iff $\sqcup\{c \mid c \; \rho \; a\} \; \rho \; a$



Origins: Hartmanis and Stearns 1964 (pair algebras); Mycroft-Jones 1986 (LU-closure); Cousot-Cousot JLC 1992; Backhouse-Backhouse 1998



Proposition: For L-U-LUB-GLB-closed $\rho \subseteq C \times A$, $C\langle \alpha_\rho, \gamma_\rho \rangle A$ is a Galois connection, where

- $\alpha_\rho(c) = \sqcap\{a \mid c \; \rho \; a\}$
- $\gamma_\rho(a) = \sqcup\{c \mid c \; \rho \; a\}$

Intuition: U-closed makes γ_ρ mono; L-closed makes α_ρ mono; GLB-closed ensures α_ρ selects the most precise sound answer; LUB-closed ensures γ_ρ selects the most general sound answer.

Note that $c \; \rho \; a$ iff $c \sqsubseteq_C \gamma_\rho a$ iff $\alpha_\rho c \sqsubseteq_A a$. Backhouse[2]: ρ is a *pair algebra*.

Proposition: For Galois connection, $C\langle \alpha, \gamma \rangle A$, define $\rho_{\alpha\gamma} \subseteq C \times A$ as $\{(c, a) \mid \alpha c \sqsubseteq a\}$. Then,

$$\rho_{\alpha\gamma} \text{ is L-U-LUB-GLB-closed and } \langle \alpha_{\rho_{\alpha\gamma}}, \gamma_{\rho_{\alpha\gamma}} \rangle = \langle \alpha, \gamma \rangle.$$

“Completing” U-GLB-closed $\rho \subseteq C \times A$ into a Galois connection between $\mathcal{P}(C)$ and A

Here is a standard technique: Let C be a (discretely ordered) set and let A be a complete lattice.

Theorem: If $\rho \subseteq C \times A$ is U-GLB-closed, then $\mathcal{P}(C)\langle \alpha_{\bar{\rho}}, \gamma_{\bar{\rho}} \rangle A$ is a Galois connection, where

- $\gamma_{\bar{\rho}}(a) = \{c \mid c \; \rho \; a\}$
- $\alpha_{\bar{\rho}}(S) = \sqcap\{a \mid S \subseteq \gamma_{\bar{\rho}} a\}$

Note that $c \; \rho \; a$ iff $c \in \gamma_{\bar{\rho}} a$ iff $\alpha_{\bar{\rho}}\{c\} \sqsubseteq a$.

The proof comes from this construction, which “completes” ρ to $\bar{\rho}$:

For $\rho \subseteq C \times A$, *define* $\bar{\rho} \subseteq \mathcal{P}(C) \times A$ *as* $S \; \bar{\rho} \; a$ *iff for all* $c \in S$, $c \; \rho \; a$.

Lemma: If ρ is U-GLB-closed, then $\bar{\rho}$ is L-U-GLB-LUB-closed, and $\gamma_{\bar{\rho}} a = \sqcup\{S \mid S \; \bar{\rho} \; a\} = \{c \mid c \; \rho \; a\}$. because $\sqsubseteq_{\mathcal{P}(C)} = \subseteq$ and $\sqcup_{\mathcal{P}(C)} = \cup$.

Example: Let Int be the discretely ordered set of integers:

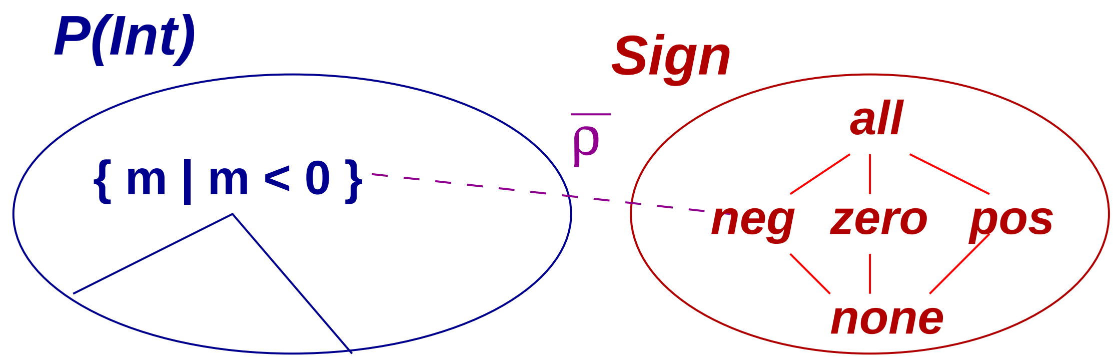
$\rho \subseteq \mathrm{Int} \times \mathit{Sign}$

$-n\ \rho\ \mathit{neg}$

$0\ \rho\ \mathit{zero}$

$+n\ \rho\ \mathit{pos}$

$n\ \rho\ \mathit{all}$



ρ is U-GLB-(and trivially, L-)closed but not LUB-closed, so it is completed to $\bar{\rho} \subseteq \mathcal{P}(\mathrm{Int}) \times \mathit{Sign}$, giving us a Galois connection, $\mathcal{P}(\mathrm{Int})\langle \alpha_{\bar{\rho}}, \gamma_{\bar{\rho}} \rangle \mathit{Sign}$.

Powersets

Powersets

When D is a partially ordered, we have choices for the "powerset" of D, but we should build a complete lattice with *singleton* and *union* operations: $(E, \sqsubseteq_E, \{\!\!\{ \cdot \}\!\!\} : D \to E, \uplus : E \times E \to E)$.

Down-set (order-ideal) completion [Cousot-Cousot ICCL94]: For $d \in D$, $S \subseteq D$, *define* $\downarrow d = \{e \in D \mid e \sqsubseteq d\}$ *and* $\downarrow S = \cup\{\downarrow d \mid d \in S\}$.

Define $\mathcal{P}_{\downarrow} D = (\{\downarrow S \mid S \subseteq D\}, \subseteq, \downarrow, \cup)$ — all down-closed subsets of D

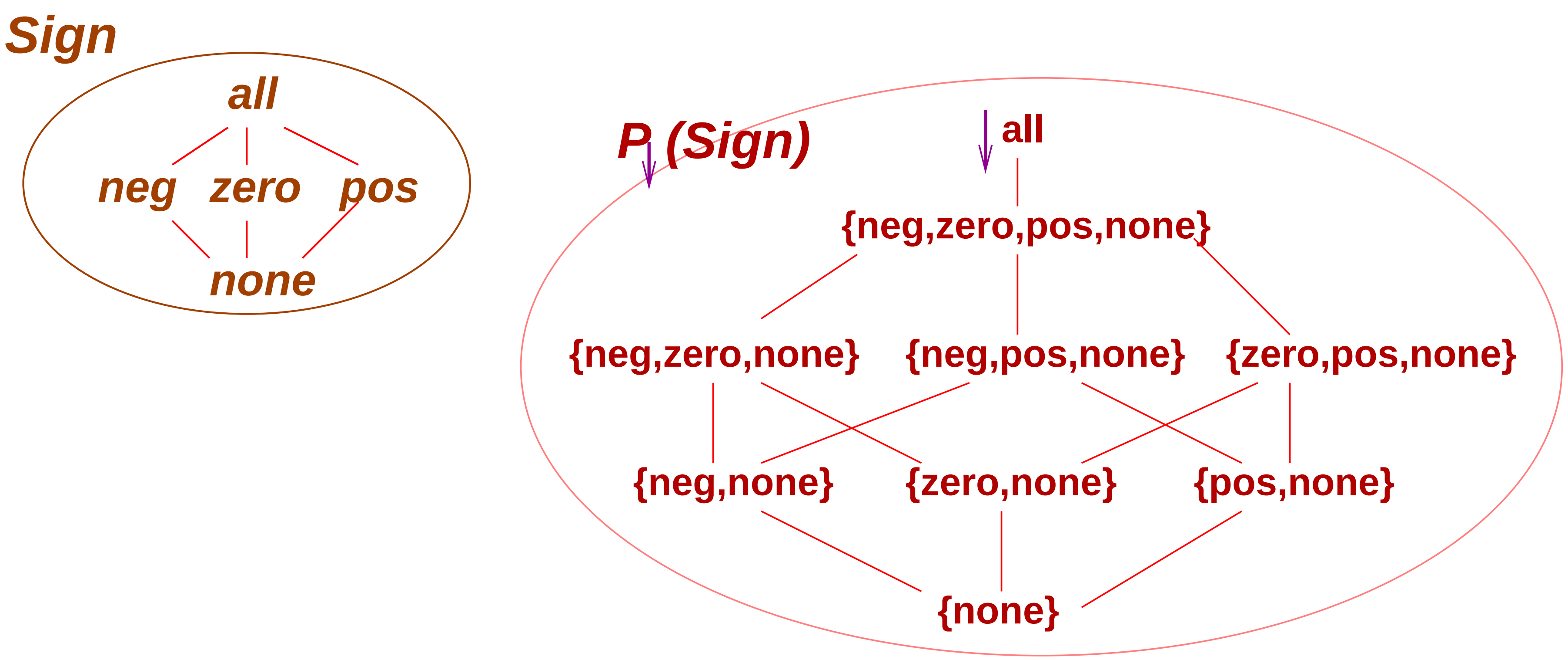
Join completion [Cousot-Cousot ICCL94] — sublattices of $\mathcal{P}_{\downarrow} D$:

$(\mathcal{M}, \subseteq, \downarrow, \sqcup_{\mathcal{M}})$, where $\mathcal{M} \subseteq \{\downarrow S \mid S \subseteq D\}$ is a *Moore family* (closed under $\cap$). *(Note that* $(\{\downarrow d \mid d \in D\}, \subseteq, \downarrow, \downarrow \circ \sqcup_D)$ *is isomorphic to* D*.)*

For every monotone $f : D \to L$, we define $\mathit{ext}(f) : \mathcal{P}_{\downarrow} D \to L$ as $\mathit{ext}(f)(S) = \sqcup_{d \in S} f(d)$.

Join completions "add new joins to D": For $\mathcal{P}(C)\langle \alpha, \gamma \rangle A$, we build $\mathcal{P}(C)\langle \bar{\alpha}, \bar{\gamma} \rangle \mathcal{P}_L A$, where $\mathcal{P}_L A$ is a join completion, $\bar{\gamma} = \mathit{ext}(\gamma)$, and $\gamma[A] \subseteq \bar{\gamma}[\mathcal{P}_L A]$.

Here is $\mathcal{S}ign$ **and its order-ideal completion:**



There is a dual construction:

Up-set (filter) completion: For $d \in D$ and $S \subseteq D$, *define* $\uparrow d = \{e \in D \mid d \sqsubseteq e\}$ *and* $\uparrow S = \cup\{\uparrow d \mid d \in S\}$.

Define $\mathcal{P}_{\uparrow} D = (\{\uparrow S \mid S \subseteq D\}, \supseteq, \uparrow, \cup)$ — all up-closed subsets of D

For every monotone $f : D \to L$, define $\mathit{ext}(f) : \mathcal{P}_{\uparrow} D \to L$ as $\mathit{ext}(f)(S) = \sqcap_{d \in S} f(d)$.

As noted in [Cousot-Cousot ICCL94], there is no obvious application of $\mathcal{P}_{\uparrow} D$ to enriching A: Given $\mathcal{P}(C)\langle\alpha, \gamma\rangle A$, we build $\mathcal{P}(C)\langle\bar{\alpha}, \bar{\gamma}\rangle \mathcal{P}_{\uparrow} A$, where $\bar{\gamma} = \mathit{ext}(\gamma)$ and we see that $\gamma[A] = \bar{\gamma}[\mathcal{P}_{\uparrow} A]$ — no “new meets” are added to A.

Fortunately, we have another use for $\mathcal{P}_{\uparrow} D$.

Lower powerdomains via Hennessy-Plotkin

Definition: For complete lattice, D, A *powerset of* D is $PD = (E, \sqsubseteq_E, \{\!|\cdot|\!\} : D \to E, \uplus : E \times E \to E)$, such that

- $(E, \sqsubseteq_E)$ is a complete lattice
- $\{\!|\cdot|\!\}$ is monotone
- $\uplus$ is monotone, absorptive, commutative, and associative
- For every monotone $f : D \to L$, there is a monotone $ext(f) : PD \to L$ such that $ext(f)\{\!|d|\!\} = f(d)$, for all $d \in D$.

For powerset PD, $d \in D$ and $S \in PD$, *define* $d\tilde{\in}S$ *iff* $\{\!|d|\!\} \uplus S = S$.

Definition: Powerset $\mathcal{P}_L D = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$ is a

- *lower powerset* iff ((for all $x\tilde{\in}S_1$, there exists $y\tilde{\in}S_2$ such that $x \sqsubseteq_\tau y$) **implies** $S_1 \sqsubseteq_E S_2$).
- *strongly* lower powerset iff **implies** is replaced by **iff**.

Proposition: For a lower powerset, $\mathcal{P}_L D$, we have that $\uplus = \sqcup$ iff $\mathcal{P}_L D$ is strongly lower.

Every join completion is a strongly lower powerset, and every strongly lower powerset, $\mathcal{P}_L D$, is order-isomorphic to its trivial join-completion, $(\{\downarrow_D S \mid S \in \mathcal{P}_L D\}, \subseteq, \downarrow_D \circ \{\!| \cdot |\!\}, \downarrow_D \circ \sqcup_D)$.

For a join completion, $d \tilde{\in} S$ iff $d \in S$.

Definition: A strongly lower powerset, $\mathcal{P}_L D$, is a *lower powerdomain* iff for every monotone $f : D \to L$, where L is itself a strongly lower powerset, $ext(f) : \mathcal{P}_L D \to L$ preserves unions (binary joins): $ext(f)(S \uplus_{\mathcal{P}_L D} S') = ext(f)(S) \uplus_L ext(f)(S')$.

When $ext(f)$ is unique, then the powerdomain is *initial*.

Lower powerdomains are stronger than what we will need, but a lower powerdomain $\mathcal{P}_L D$ has the precision expected of a "all subsets of D" construction. For example, if we defi ne $ext(f)(S) = \sqcup_{d \tilde{\in} S} f(d)$, then union-preservation is implied by $d \tilde{\in} S \sqcup S'$ iff $d \tilde{\in} S$ or $d \tilde{\in} S'$.

Upper powersets

As [Plotkin Pisa] notes, the definitions of upper powerset and strongly upper powerset coincide, so

Definition: Powerset $\mathcal{P}_U D = (E, \sqsubseteq_E, \{\!|\cdot|\!\}, \uplus)$ is an *upper powerset* iff ($S_1 \sqsubseteq_E S_2$ iff for all $y \tilde{\in} S_2$, there exists $x \tilde{\in} S_1$ such that $x \sqsubseteq_\tau y$).

$\mathcal{P}_\uparrow D$ is an upper powerset.

Proposition: For an upper powerset, $\uplus = \sqcap$.

Definition: An upper powerset, $\mathcal{P}_U D$, is an *upper powerdomain* iff for every monotone $f : D \to L$, where L is itself an upper powerset, $ext(f) : \mathcal{P}_U D \to L$ preserves unions:
$ext(f)(S \uplus_{\mathcal{P}_U D} S') = ext(f)(S) \uplus_L ext(f)(S')$.

For example, if we defi ne $ext(f)(S) = \sqcap_{d \tilde{\in} S} f(d)$, then union-preservation is implied by $d \tilde{\in} S \sqcap S'$ iff $d \tilde{\in} S$ or $d \tilde{\in} S'$.

Logical relations

Logical relations

We now attach typings to the relations. Given this grammar of types,

$$\tau ::= b \mid \tau_1 \to \tau_2 \mid \mathcal{P}_L\tau \mid \mathcal{P}_U\tau \mid \bar{\tau}$$

We will see that $\rho_{\bar{\tau}} \subseteq \mathcal{P}(C) \times A$ comes from $\rho_\tau \subseteq C \times A$

let A_τ be a complete lattice of the appropriate form (e.g., $A_{\tau_1 \to \tau_2}$ is a domain of monotone functions, $A_{\mathcal{P}_U\tau}$ is an upper powerset, etc.)

We define this family of logical relations, $\rho_\tau \subseteq C_\tau \times A_\tau$*:*

ρ_b is given

$f \; \rho_{\tau_1 \to \tau_2} \; f^\sharp$ iff for all $c \in C_{\tau_1}, a \in A_{\tau_1}, c \; \rho_{\tau_1} \; a$ implies $f(c) \; \rho_{\tau_2} \; f^\sharp(a)$

$S \; \rho_{\mathcal{P}_L\tau} \; T$ iff for all $c \tilde{\in} S,$ there exists $a \tilde{\in} T$ such that $c \; \rho_\tau \; a$

$S \; \rho_{\mathcal{P}_U\tau} \; T$ iff for all $a \tilde{\in} T,$ there exists $c \tilde{\in} S$ such that $c \; \rho_\tau \; a$

$S \; \rho_{\bar{\tau}} \; a$ iff for all $c \in S, c \; \rho_\tau \; a$

and use it to generate Galois connections inductively.

Simulation relations are just logical relations

Binary relations are the key component in simulation proofs:

For $\rho \subseteq C \times A$, transition relations, $R \subseteq C \times C$, $R^\sharp \subseteq A \times A$,

Definition: $R^\sharp$ *simulates* R (*or,* $R^\sharp$ *overapproximates* R), written $R \lhd_\rho R^\sharp$, iff for all $c, c' \in C, a \in A$,

$c \; \rho \; a$ and $c \; R \; c'$ imply there exists $a' \in A$ such that $a \; R^\sharp \; a'$ and $c' \; \rho \; a'$.

Say that we represent R and $R^\sharp$ as multi-functions, $R : C \rightarrow \mathcal{P}_L C$ and $R^\sharp : A \rightarrow \mathcal{P}_L A$:

Theorem: $R \lhd_{\rho_b} R^\sharp$ iff $R \; \rho_{b \rightarrow \mathcal{P}_L b} \; R^\sharp$. The proof assumes that R and $R^\sharp$ behave monotonically, which is not a restriction, given that C is typically discretely ordered and $R^\sharp$ must be monotone to be computed with the standard techniques.

The dual simulation, $R^\flat \lhd_{\rho_b^{-1}} R$, is characterized as $R \; \rho_{b \rightarrow \mathcal{P}_U b} \; R^\flat$. ($R^\flat$ *underapproximates* R.)

The results that follow

1. Every (U-GLB-...-closed) family of logical relations, $\rho_\tau \subseteq C_\tau \times A_\tau$, inductively lift to a family of Galois connections whose targets are A_τ. Specifically, simulation is an instance of an "inductively defined" Galois connection.

2. Dams's best simulations coincide with the best abstract transition functions defined by the Galois connections.

3. The family of logical relations define a *validation logic*, such that $a \models_\tau \phi$ *and* $a \, \rho_\tau \, c$ *imply* $c \models_\tau \phi$, as well as a dual *refutation logic* (explained later). Thus, description logic and Hennessy-Milner logic are instances of the validation logic.

Related results from [*Loiseaux, et al. 95*]

For *sets* C and A and $\rho \subseteq C \times A$, $\mathcal{P}(C)\langle \mathrm{post}[\rho], \widetilde{\mathrm{pre}}[\rho]\rangle \mathcal{P}(A)$ is a Galois connection.

Note that $\widetilde{\mathrm{pre}}[\rho] = \lambda T.\{c \mid c.\rho \subseteq T\}$ is ρ "reduced" to an underapproximation function.

$\mathrm{post}[\rho] = \lambda S.\{a \mid$ exists $c \in S, c\,\rho\,a\}$. A's partial ordering, if any, is forgotten.

For $R \subseteq C \times C$, $R^\sharp \subseteq A \times A$, simulation is equivalently defined

$$R \textit{ is } \rho\textit{-simulated by } R^\sharp \textit{ iff } R^{-1} \cdot \rho \subseteq \rho \cdot (R^\sharp)^{-1}$$

Treating R^{-1} and $(R^\sharp)^{-1}$ as functions, define soundness as

$$(R^\sharp)^{-1} \textit{ is a sound overapproximation for } R^{-1} \textit{ with respect to } \gamma \textit{ iff}$$
$$\mathrm{pre}[R] \circ \gamma \sqsubseteq_{\mathcal{P}(A) \to \mathcal{P}(C)} \gamma \circ \mathrm{pre}[R^\sharp]$$

For ρ, R, $R^\sharp$, Loiseaux, et al. prove

- R is ρ-simulated by $R^\sharp$ iff $(R^\sharp)^{-1}$ is sound for R^{-1} w.r.t. $\widetilde{\mathrm{pre}}[\rho]$.
- and so, $a \models \phi \in ACTL$ implies $c \models \phi$, for $c\,\rho\,a$.

Base types, b: *manufacturing* $\rho_b \subseteq C \times A$

When starting from a (discretely ordered) set C, of type b, and a complete lattice A, it is highly unlikely that $\rho_b \subseteq C \times A$ is LUB-closed (because C has no lubs for distinct elements).

LUB-closure means that each $a \in A$ has a best concretization in C. To have this, we usually must “complete” C.

Complete the relation to $\rho_{\bar{b}} \subseteq \mathcal{P}(C) \times A$, giving $\mathcal{P}(C)\langle \alpha_{\rho_{\bar{b}}}, \gamma_{\rho_{\bar{b}}} \rangle A$, where, for $c \in C$ and $a \in A$, $c\ \rho_b\ a$ iff $\alpha_{\rho_{\bar{b}}}\{c\} \sqsubseteq a$.

Even when C is a complete lattice, it is diffi cult to defi ne a LUB-closed $\rho_b \subseteq C \times A$ (generally, $c\ \rho_b\ a$ and $c'\ \rho_b\ a$ do not imply $c \sqcup c'\ \rho_b\ a$). For example, $C = Nat_{\bot}^{\top}$, $A = \{even, odd, \bot, \top\}$, $2\ \rho\ even$ and $4\ \rho\ even$, but $\neg(\top\ \rho\ even)$.

Preview of closure properties on relations of compound type

$f \; \rho_{\tau_1 \to \tau_2} \; f^\sharp$ iff for all $c \in C_{\tau_1}, a \in A_{\tau_1}, c \; \rho_{\tau_1} \; a$ implies $f(c) \; \rho_{\tau_2} \; f^\sharp(a)$

$S \; \rho_{\mathcal{P}_L \tau} \; T$ iff for all $c \tilde{\in} S,$ there exists $a \tilde{\in} T$ such that $c \; \rho_\tau \; a$

$S \; \rho_{\mathcal{P}_U \tau} \; T$ iff for all $a \tilde{\in} T,$ there exists $c \tilde{\in} S$ such that $c \; \rho_\tau \; a$

$S \; \rho_{\bar{\tau}} \; a$ iff for all $c \in S, c \; \rho_\tau \; a$

For $\rho_\tau \subseteq C \times A$ and for $F[\tau] \in \{\tau' \to \tau, \; \mathcal{P}_L \tau, \; \mathcal{P}_U \tau, \; \bar{\tau}\}$,

If ρ_τ is L-closed, then so is $\rho_{F[\tau]}$.

If ρ_τ is U-closed, then so is $\rho_{F[\tau]}$.

If ρ_τ is U-GLB-closed, then so are $\rho_{\tau' \to \tau}$, $\rho_{\bar{\tau}}$, and $\rho_{\mathcal{P}_L \tau}$.

If ρ_τ is L-LUB-closed, then so are $\rho_{\tau' \to \tau}$ and $\rho_{\mathcal{P}_U \tau}$.

Relation to [*Backhouse*^{2} *1998*]

A relational formulation of [Hartmanis and Stearns 1964] and [Abramsky 1990]:

$\rho \subseteq C \times A$ is a *pair algebra* iff exist $\alpha : C \rightarrow A$ and $\gamma : A \rightarrow C$ s.t.

$$\{(c,a) \mid \alpha c \sqsubseteq_A a\} = \rho = \{(c,a) \mid c \sqsubseteq_C \gamma a\}$$

For the category, $\mathcal{C}$, of partially ordered sets *(objects)* and binary relations *(morphisms)*, *if* an endofunctor, $\sigma : \mathcal{C} \Rightarrow \mathcal{C}$, is also

1. *monotonic*: for relations, $R, S \subseteq C \times C'$, $R \subseteq S$ implies $\sigma R \subseteq \sigma S$
2. *invertible*: for all relations, $R \subseteq C \times C'$, $(\sigma R)^{-1} = \sigma(R^{-1})$,

then σ maps pair algebras to pair algebras, that is, σ *is a unary type constructor that "lifts" a Galois connection between* C *and* A *to one between* σC *and* σA*.*

The result generalizes to n-ary functors and applies to the standard functors, $\tau \times \tau$, $\tau \rightarrow \tau$, $\mathrm{List}(\tau)$, etc.

But the result does not apply to $\mathcal{P}_L\tau$ *nor* $\mathcal{P}_U\tau$ *— invertibility* (2) *fails.*

Function spaces: *from* $\rho_{\tau_1} \subseteq C_1 \times A_1$ *and* $\rho_{\tau_1} \subseteq C_2 \times A_2$ *to* $\rho_{\tau_1 \to \tau_2} \subseteq (C_1 \to C_2) \times (A_1 \to A_2)$

For abstract complete lattices, A_1 and A_2, let Let $A_1 \to A_2$ denote the complete lattice of *monotone* (not necessarily Scott-continuous) functions with the usual pointwise ordering.

Let $\rho_{\tau_i} \subseteq C_{\tau_i} \times A_{\tau_i}$, $i \in 1..2$, be U-GLB-L-LUB-closed. Recall that

$$f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp \textit{ iff for all } c \in C_{\tau_1}, a \in A_{\tau_1}, c \, \rho_{\tau_1} \, a \textit{ implies } f(c) \, \rho_{\tau_2} \, f^\sharp(a).$$

Proposition: For $f : C_{\tau_1} \to C_{\tau_2}$, $f^\sharp : A_{\tau_1} \to A_{\tau_2}$,

$$f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp \text{ iff } \alpha_{\rho_{\tau_2}} \circ f \sqsubseteq_{A_1 \to A_2} f^\sharp \circ \alpha_{\rho_{\tau_1}}$$

$$f^\sharp{}_{best}(a) = \alpha_{\rho_{\tau_2}} \circ f \circ \gamma_{\rho_{\tau_1}} = \sqcap\{a' \mid f(\sqcup\{c \mid c \, \rho_{\tau_1} \, a\}) \, \rho_{\tau_2} \, a'\}$$

We can generate higher-order Galois connections of form

$C_1 \to C_2 \langle \alpha, \gamma \rangle A_1 \to A_2$ and $\mathcal{P}_\downarrow(C_1 \to C_2) \langle \alpha^\phi, \gamma^\phi \rangle A_1 \to A_2$

from $\rho_{\tau_1 \to \tau_2}$ and $\rho_{\tau_1 \Rightarrow \tau_2}$, respectively. See [Cousot-Cousot-ICCL94].

Completed sets: *from* $\rho_\tau \subseteq C \times A$ *to* $\rho_{\bar\tau} \subseteq \mathcal{P}_L C \times A$

We have $\rho_\tau \subseteq C \times A$. Recall, for join completion $\mathcal{P}_L C$ and $\rho_{\bar\tau} \subseteq \mathcal{P}_L C \times A$, that $S\, \rho_{\bar\tau}\, a$ iff for all $c \in S$, $c\, \rho_\tau\, a$.

Proposition: $\rho_{\bar\tau}$ is U-closed when ρ_τ is; it is GLB-closed when ρ_τ is U-GLB-closed; and it is L-closed when ρ_τ is.

When $\rho_\tau \subseteq C \times A$ is U-GLB-L-closed, then $\rho_{\bar\tau} \subseteq \mathcal{P}_\downarrow C \times A$ is U-GLB-L-LUB-closed.

Sometimes LUB-closure of $\rho_{\bar\tau}$ comes from a weaker join completion:

Proposition: For $a \in A$, let $\mathcal{L}_a = \{S \in \mathcal{P}_L C \mid S\, \rho_{\bar\tau}\, a\}$. If *(i)* ρ_τ is L-LUB-closed, and *(ii)* for all $c \in \sqcup \mathcal{L}_a$, there is some $S_c \subseteq \cup \mathcal{L}_a$ such that $c = \sqcup S_c$, *then* $\rho_{\bar\tau}$ is LUB-closed.

Item *(ii)* says that every element, $c \in \sqcup \mathcal{L}_a$, is a join of elements that are related to a. By L-LUB closure of ρ_τ, we get $c\, \rho_\tau\, a$. This idea reappears for lower powersets.

Lower powersets: *from* $\rho_\tau \subseteq C \times A$ *to* $\rho_{\mathcal{P}_L\tau} \subseteq \mathcal{P}_L C \times \mathcal{P}_L A$

Let PC be a powerset for C and let $\mathcal{P}_L A$ be a strongly lower powerset for A. Let $\rho_\tau \subseteq C \times A$.

Recall, for $S \in PC$, $T \in \mathcal{P}_L A$, that $S\, \rho_{\mathcal{P}_L\tau}\, T$ iff for all $c \tilde{\in} S$, there exists $a \tilde{\in} T$ such that $c\, \rho_\tau\, a$. — Every $c \tilde{\in} S$ is approximated by some $a \tilde{\in} T$.

Proposition: $\rho_{\mathcal{P}_L\tau}$ is U-closed if ρ_τ is; it is GLB-closed if ρ_τ is; it is L-closed if PC is a strongly lower powerset.

Proposition: For all C and A, $\rho_{\mathcal{P}_L\tau} \subseteq \mathcal{P}_\downarrow C \times \mathcal{P}_L A$ is L-LUB-closed.

because $\sqcup = \cup$.

So, we can always begin play with a U-GLB closed $\rho_b \subseteq C \times A$ and lift it to U-GLB-L-LUB-closed $\rho_{\mathcal{P}_L b} \subseteq \mathcal{P}_\downarrow C \times \mathcal{P}_L A$.

LUB-closure of $\rho_{\mathcal{P}_L \tau}$ is not guaranteed from ρ_τ, but we have

Proposition: For all $T \in \mathcal{P}_L A$, let $\mathcal{L}_T = \{S \in PC \mid S\, \rho_{\mathcal{P}_L \tau}\, T\}$. If

1. ρ_τ is L-LUB-closed
2. for all $c \tilde{\in} \sqcup \mathcal{L}_T$, there exists $a \tilde{\in} T$ such that $c = \sqcup S_a$, where $S_a \subseteq \{c' \tilde{\in} S \in \mathcal{L}_T \mid c'\, \rho_\tau\, a\}$

then $\rho_{\mathcal{P}_L \tau}$ is LUB-closed.

Item 2 says that every element, $c \tilde{\in} \sqcup \mathcal{L}_T$, is a join of elements that are related to some $a \tilde{\in} T$. By L-LUB closure of ρ_τ, we get $c\, \rho_\tau\, a$. This property is fulfi lled, for example, by the Scott-closed-set lower powerdomain construction.

Dams's results

Synthesizing a most-precise simulation

In his thesis, Dams proves, for Galois connection $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$ and transition relation $R \subseteq C \times C$, that the most precise, sound abstract transition relation $R \subseteq A \times A$ is

$$R(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in min\{S' \mid R^{\exists\exists}(\gamma(a), S')\}\}$$

Recoded as a function and simplified, this reads

$$R(a) = \{\alpha(s') \mid \exists s \in \gamma(a), s' \in R(s)\}$$

Our machinery gives us the same result: Given U-GLB-closed $\rho_b \subseteq C \times A$ and transition function $R : C \to \mathcal{P}(C)$, we generate $\rho_{\bar{b}\to\mathcal{P}_L b}$ and synthesize the most precise, sound abstract transition function, $R^\sharp : A \to \mathcal{P}_L A$, such that $ext_{\bar{b}}(R)\ \rho_{\bar{b}\to\mathcal{P}_L b}\ R^\sharp$:

$$R^\sharp(a) = (\alpha_{\rho_{\mathcal{P}_L b}} \circ ext_{\bar{b}}(R) \circ \gamma_{\rho_{\bar{b}}})(a) = \sqcup\{\{\!|\alpha_{\rho_{\bar{b}}}\{s'\}|\!\} \mid \exists s \in \gamma_{\rho_{\bar{b}}}(a), s' \in R(s)\}$$

Upper powersets: *from* $\rho_\tau \subseteq C \times A$ *to* $\rho_{\mathcal{P}_U\tau} \subseteq \mathcal{P}_U C \times \mathcal{P}_U A$

Let PC be a powerset and $\mathcal{P}_U A$ be an upper powerset, for C and A, respectively. Let $\rho_\tau \subseteq C \times A$. Recall, for $S \tilde{\in} PC$, $T \tilde{\in} \mathcal{P}_U A$, that $S \, \rho_{\mathcal{P}_U\tau} \, T$ iff for all $a \tilde{\in} T$, there exists $c \tilde{\in} S$ such that $c \, \rho_\tau \, a$.

Proposition: $\rho_{\mathcal{P}_U\tau}$ is U-closed when ρ_τ is; it is LUB-closed when ρ_τ is; it is L-closed when PC is an upper powerset.

Proposition: For all $S \in PC$, let $\mathcal{G}_S = \{T \in \mathcal{P}_U A \mid S \, \rho_{\mathcal{P}_U\tau} \, T\}$. If

1. ρ_τ is U-GLB-closed
2. for all $a \tilde{\in} \sqcap_{\mathcal{P}_U A} \mathcal{G}_S$, there exists $c \tilde{\in} S$ such that $a = \sqcap_A T_c$, where $T_c \subseteq \{a' \tilde{\in} T \in \mathcal{G}_S \mid c \, \rho_\tau \, a'\}$

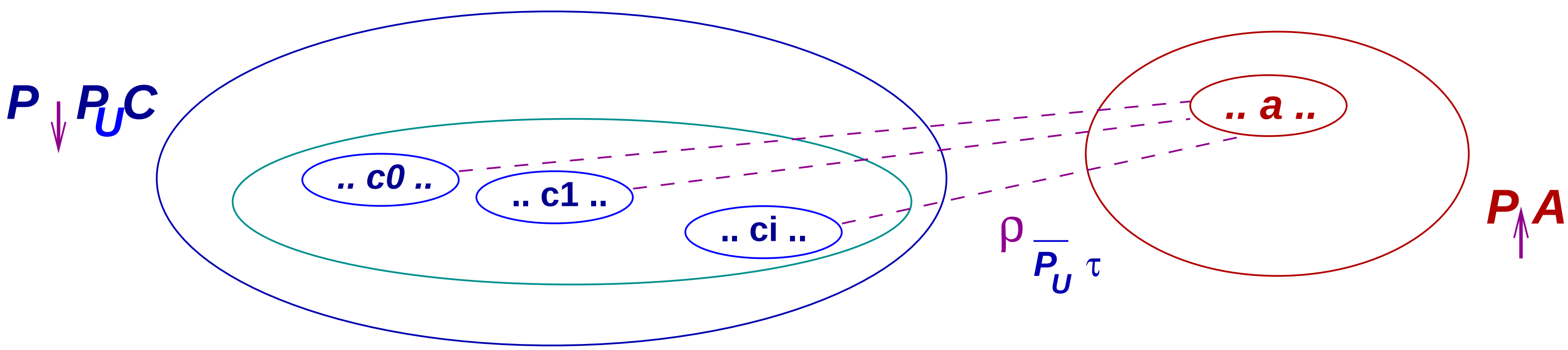
then $\rho_{\mathcal{P}_U\tau}$ is GLB-closed.

Corollary: Let upper powerset $\mathcal{P}_\uparrow A = (\{\uparrow D \mid D \subseteq A\}, \supseteq, \uparrow, \cup)$. Then $\rho_{\mathcal{P}_U\tau} \subseteq PC \times \mathcal{P}_\uparrow A$ is GLB-closed. because $\sqcap = \cup$.

Overapproximating underapproximated sets

There is a good use for $\rho_{\mathcal{P}_{\mathrm{U}}\tau}$: defining an *overapproximation analysis of underapproximations.*

Consider $\rho_{\bar{\mathcal{P}}_{\mathrm{U}}\tau} \subseteq \mathcal{P}_{\downarrow}(\mathcal{P}_{\mathrm{U}}C) \times \mathcal{P}_{\mathrm{U}}A$; it says that $\bar{S}\, \rho_{\bar{\mathcal{P}}_{\mathrm{U}}\tau}\, T$ iff for each set $S \in \bar{S}$, $S\, \rho_{\mathcal{P}_{\mathrm{U}}\tau}\, T$, that is, T underapproximates each $S \in \bar{S}$:



We can readily construct $\rho_{\bar{\mathcal{P}}_{\mathrm{U}}\tau}$:

1. define a U-GLB-closed $\rho_{\tau} \subseteq C \times A$;
2. lift it to a U-L-GLB-closed $\rho_{\mathcal{P}_{\mathrm{U}}\tau} \subseteq \mathcal{P}_{\mathrm{U}}C \times \mathcal{P}_{\uparrow}A$;
3. complete it to a U-GLB-L-LUB-closed $\rho_{\bar{\mathcal{P}}_{\mathrm{U}}\tau} \subseteq \mathcal{P}_{\downarrow}(\mathcal{P}_{\mathrm{U}}C) \times \mathcal{P}_{\uparrow}A$.

The resulting Galois connection is

$$\alpha_{\rho_{\bar{\mathcal{P}}_{\mathrm{U}}\,\tau}}\,\bar{S} = \sqcap\{\mathsf{T} \in \mathcal{P}_{\uparrow}A \mid \text{ for all } S \in \bar{S}, S\ \rho_{\mathcal{P}_{\mathrm{U}}\,\tau}\ \mathsf{T}\}$$

$$\gamma_{\rho_{\bar{\mathcal{P}}_{\mathrm{U}}\,\tau}}\,\mathsf{T} = \{S \mid S\ \rho_{\mathcal{P}_{\mathrm{U}}\,\tau}\ \mathsf{T}\}$$

Example: We complete $\rho : \mathrm{Nat} \times \mathrm{Polarity} = \{\mathrm{none}, \mathrm{even}, \mathrm{odd}, \mathrm{any}\}$ and obtain $\gamma : \mathcal{P}_{\uparrow}\mathrm{Polarity} \to \mathcal{P}_{\downarrow}(\mathcal{P}(\mathrm{Nat})^{\mathrm{op}})$:

$\gamma\{\} =$ all subsets of nats

$\supseteq$

$\gamma\{\mathrm{any}\} =$ nonempty subsets of nats

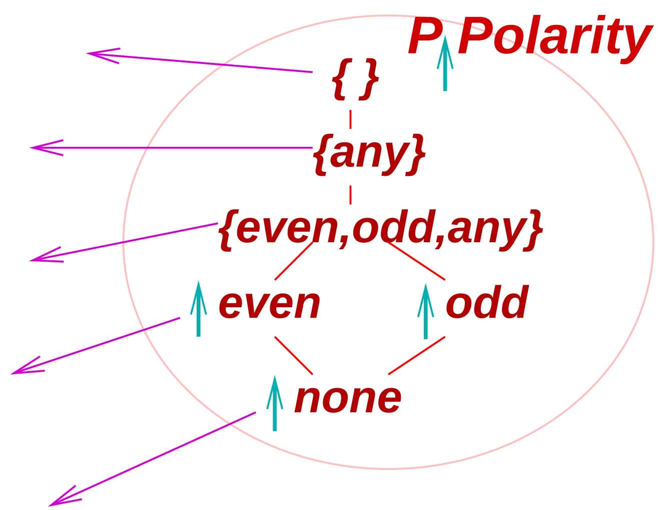
$\supseteq$

$\gamma\{\mathrm{even}, \mathrm{odd}, \mathrm{any}\} =$ all sets with 1+ even and 1+ odd $\supseteq$

$\gamma \uparrow\mathrm{even} =$ all sets with 1+ even

$\supseteq$

$\gamma \uparrow\mathrm{none} =$ empty set



Synthesizing a most-precise dual simulation

Dams proves, for Galois connection $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$ and $R \subseteq C \times C$, that the best underapproximating relation $R \subseteq A \times A$ is

$$R(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in \min\{S' \mid R^{\forall\exists}(\gamma(a), S')\}\}$$

Recoded as a function and simplified, this reads

$$R(a) = \{\alpha(Y) \mid Y \in \min\{S' \mid \text{for all } s \in \gamma(a), R(s) \cap S' \neq \{\}\}\}$$

Our machinery gives us the same result:

Given U-GLB-closed $\rho_b \subseteq C \times A$ and transition function $R : C \to \mathcal{P}(C)$, we generate $\rho_{\bar{b}\to\bar{\mathcal{P}}_U b} \subseteq (\mathcal{P}(C) \to \mathcal{P}_\downarrow(\mathcal{P}(C)^{op})) \times (A \to \mathcal{P}_\uparrow A)$.

We generate this most precise, sound underapproximating abstract transition function, $R^\flat : A \to \mathcal{P}_\uparrow A$:

$$R^\flat(a) = (\alpha_{\rho_{\bar{\mathcal{P}}_U b}} \circ ext(\{\!\!\{ \cdot \}\!\!\} \circ R^{op}) \circ \gamma_{\rho_{\bar{b}}})(a)$$

where $\{\!\!\{ \cdot \}\!\!\} \circ R^{op} : C \to \mathcal{P}_{\downarrow}\mathcal{P}(C)^{op}$ is $(\{\!\!\{ \cdot \}\!\!\} \circ R^{op})(c) = \uparrow R(c) = R(c)$,

and $ext(\{\!\!\{ \cdot \}\!\!\} \circ R^{op}) : \mathcal{P}(C) \to \mathcal{P}_{\downarrow}(\mathcal{P}(C)^{op})$ is
$ext(\{\!\!\{ \cdot \}\!\!\} \circ R^{op})(S) = \downarrow_{\mathcal{P}(C)^{op}} \{R(c) \mid c \in S\} = \{S \supseteq R(c) \mid c \in S\}$

and $\alpha_{\rho_{\bar{\mathcal{P}}_U b}}(\bar{S}) = \sqcap\{T \mid \text{for all } S \in \bar{S}, S\ \rho_{\mathcal{P}_U b}\ T\}$.

That is, $ext(\{\!\!\{ \cdot \}\!\!\} \circ R^{op})$ maps a set of arguments to the set of sets of answers, and $\alpha_{\bar{\rho}_{\mathcal{P}_U b}}$ produces the smallest abstract set that underapproximates every answer set $R(c)$, for $c \in \gamma_{\bar{\rho}_b}(a)$. We take into account that A is partially ordered.

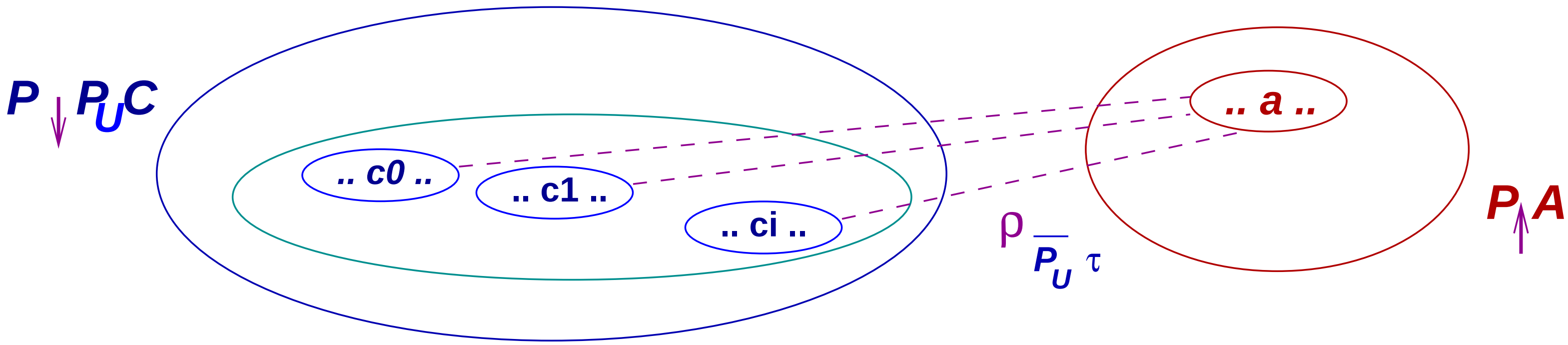
Simplifi ed,
$R^{\flat}(a) = \sqcap\{T \in \mathcal{P}_{\uparrow}A \mid \text{for all } a' \in T, \text{for all } s \in \gamma_{\rho_{\bar{b}}}(a), R(s) \cap \gamma_{\rho_{\bar{b}}}(a') \neq \{\}\}$

is provably equal to Dams's defi nition:

$$R(a) = \{\alpha(Y) \mid Y \in min\{S' \mid \text{for all } s \in \gamma(a), R(s) \cap S' \neq \{\}\}\}$$

We can show that $R(a)$ belongs to and is $\sqsubseteq$ all elements in the former set.

Every answer set is kept distinct and each set's elements are underapproximated:



Dual simulation lifts to sets of arguments:

Theorem: $R^\flat \lhd_{\rho^{-1}} R$ iff $R \, \rho_{b \to \mathcal{P}_U b} \, R^\flat$ iff $ext(\{\!| \cdot |\!\} \circ R^{op}) \, \rho_{\bar{b} \to \bar{\mathcal{P}}_U b} \, R^\flat$

Validation and refutation logics

A logic generated from the logical relations

We define this language of assertions,

$$\phi ::= p_b \mid f.\phi \mid \forall\phi \mid \exists\phi$$

and this semantics of typed judgements for both concrete domains, C_τ, and abstract domains, A_τ:

$d \models_b p_b$ is given, for $d \in D_b$

$d \models_{\tau_1 \to \tau_2} f.\phi$ if $f(d) \models_{\tau_2} \phi$, for $d \in D_{\tau_1}, f \in D_{\tau_1 \to \tau_2}$

$S \models_{\mathcal{P}_L \tau} \forall\phi$ if for all $d \tilde{\in} S, d \models_\tau \phi$, for $S \in D_{\mathcal{P}_L \tau}$

$S \models_{\mathcal{P}_U \tau} \exists\phi$ if there exists $d \tilde{\in} S$ such that $d \models_\tau \phi$, for $S \in D_{\mathcal{P}_U \tau}$

For abstract values, the typed judgement for $\bar{\tau}$ reads

$$a \models_{\bar{\tau}} \phi \text{ if } a \models_\tau \phi, \text{ for } a \in A_\tau.$$

but for concrete values, it must read

$$S \models_{\bar{\tau}} \phi \text{ if } c \models_\tau \phi, \text{ for all } c \in S, S \in \mathcal{P}_L C_\tau \text{ (a join completion)}$$

Some “syntactic sugar”:

$$d \models \forall R\phi \text{ (that is, } d \models \Box\phi\text{) abbreviates } d \models_{\tau_1 \to \mathcal{P}_L \tau_2} R.\forall\phi$$

$$d \models \exists R\phi \text{ (} d \models \Diamond\phi\text{) abbreviates } d \models_{\tau_1 \to \mathcal{P}_U \tau_2} R.\exists\phi$$

This reveals that the logic extracted from the logical relations is a variant of Hennessy-Milner or description logic.

$\tau ::= b \mid \tau_1 \to \tau_2 \mid \mathcal{P}_L\tau \mid \mathcal{P}_U\tau \mid \bar{\tau}$

Assume, for all function symbols, f, typed $\tau_1 \to \tau_2$, there are interpretations $f : C_{\tau_1} \to C_{\tau_2}$, and $f^\sharp : A_{\tau_1} \to A_{\tau_2}$, such that $f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp$. Also, we formalize when judgements $a \models_\tau \phi$ are *well formed* — see the typings on $a \in A_{\tau'}$ in the defi nitions of $\models_\tau \phi$

Definition: $\models_\tau \phi$ *is* ρ_τ*-sound* iff for all $c \in C_{\tau_1}$, $a \in A_{\tau_2}$,

$a \models_\tau \phi$ is well formed, holds true, and $c \, \rho_\tau \, a$ imply $c \models_\tau \phi$.

Assume that all $\models_b p$ are ρ_b-sound.

Theorem: For all types, τ, we have that $\models_\tau \phi$ are ρ_τ-sound.

We can add the logical connectives,

$$d \models_\tau \phi_1 \wedge \phi_2 \text{ if } d \models_\tau \phi_1 \text{ and } d \models_\tau \phi_2$$

$$d \models_\tau \phi_1 \vee \phi_2 \text{ if } d \models_\tau \phi_1 \text{ or } d \models_\tau \phi_2$$

and prove these ρ_τ-sound.

Validating $\neg\phi$ requires a *refutation logic*

Define $c \models_\tau \neg\phi$ *iff* $c \not\models_\tau \phi$.

We have a logic that validates ϕ for $c \in C$ by validating it for $a \in A$, so we might have also a logic that *refutes* properties similarly:

Read $a \models_\tau^{\neg pos} \phi$ as "it is not possible that any value modelled by a has property ϕ."

$$a \models_b^{\neg pos} p \text{ is given, for } a \in A_b$$

$$a \models_{\tau_1 \to \tau_2}^{\neg pos} f.\phi \text{ if } f(a) \models_{\tau_2}^{\neg pos} \phi, \text{ for } a \in A_{\tau_1}, f \in A_{\tau_1 \to \tau_2}$$

$$T \models_{\mathcal{P}_U \tau}^{\neg pos} \forall\phi \text{ if exists } a \tilde{\in} T, a \models_\tau^{\neg pos} \phi, \text{ for } T \in A_{\mathcal{P}_U \tau}$$

$$T \models_{\mathcal{P}_L \tau}^{\neg pos} \exists\phi \text{ if for all } a \tilde{\in} T, a \models_\tau^{\neg pos} \phi, \text{ for } T \in A_{\mathcal{P}_L \tau}$$

$$a \models_{\bar{\tau}}^{\neg pos} \phi \text{ if } a \models_\tau^{\neg pos} \phi, \text{ for } a \in A_\tau$$

Definition: $\models_\tau^{\neg pos} \phi$ is ρ_τ-*sound* iff for all $c \in C_{\tau_1}$, $a \in A_{\tau_2}$, $a \models_\tau^{\neg pos} \phi$ is well formed, holds, and $c \; \rho_\tau \; a$ imply $c \not\models_\tau \phi$.

Theorem: All $\models_\tau^{\neg pos} \phi$ are ρ_τ-sound.

The case for $\models_{\tau}^{\neg pos}$ ϕ shows signifi cant loss of precision: $a \models_{\tau}^{\neg pos} \phi$ and $S\ \rho_{\tau}\ a$ imply *for all* $c \in S$, that $c \models_{\tau}^{\neg pos} \phi$, whereas we need only show that *there exists* some $c \in S$, such that $c {\models^{\neg pos}}_{\tau} \phi$.

Corollary: $a \models_{\tau} \neg\phi$ *if* $a \models_{\tau}^{\neg pos} \phi$ is sound for ρ_{τ}.

$a \models_{\tau}^{\neg pos} \neg\phi$ *if* $a \models_{\tau} \phi$ is sound for ρ_{τ}.

In the refutation logic, $\models_{\tau}^{\neg pos} \phi$, the roles of $\mathcal{P}_L\tau$ and $\mathcal{P}_U\tau$ are exchanged. This, as well as the need to validate a mix of $\forall$ and $\exists$, means we must employ $R^{\sharp}$ and $R^{\flat}$ to validate/refute assertions — this is the idea behind mixed/modal transition systems.

The Sagiv-Reps-Wilhelm TVLA system simultaneously calculates validation and refutation logics.

We might approximate every concrete set by a *pair* of lower and upper approximations: $\rho_{P\tau} \subseteq PC \times (\mathcal{P}_L A \times \mathcal{P}_U A)$. This motivates sandwich- and mixed-powerdomains for over-under-approximation of sets [Huth-Jagadeesan-Schmidt].

References

Primary:

1. This talk: `www.cis.ksu.edu/~schmidt/papers`
2. K. Backhouse and R. Backhouse. Galois Connections and Logical Relations. Mathematics of Program Construction, LNCS 2386, 2002.
3. P. Cousot and R.Cousot. Abstract interpretation frameworks. *Journal of Logic and Computation* 2 (1992).
4. P. Cousot and R.Cousot. Higher-order abstract interpretation. IEEE Conf. on Computer Languages, 1994.
5. D. Dams. Abstract interpretation and partition refi nement for model checking. PhD thesis, Univ. Eindhoven, 1996.
6. C. Loiseaux, et al. Property preserving abstractions for the verifi cation of concurrent systems. *Formal Methods in System Design* 6 (1995).
7. A. Mycroft and N.D. Jones. A relational framework for abstract interpretation. In Programs as Data Objects, LNCS 217, 1985.
8. G. Plotkin. Domain theory. Lecture notes, Univ. Pisa 1982.

Secondary:

1. S. Abramsky, Abstract interpretation, logical relations, and Kan extensions. *J. Logic and Computation* 1 (1990).
2. F. Baader, et al. *The Description Logic Handbook.* Cambridge Univ. Press 2003.
3. D. Dams, R. Gerth, O. Grumberg. Abstract Interpretation of Reactive Systems. *ACM TOPLAS* 19 (1997).
4. J. Hartmanis and R. Stearns. Pair algebras and their application to automata theory. *Information and Control* 7 (1964).
5. R. Heckman. *Powerdomain constructions.* PhD thesis, Saarbrücken, 1990.
6. M. Huth, R. Jagadeesan, D. Schmidt. Modal transition systems: a foundation for three-valued program analysis, ESOP 2002. Also, A domain equation for refi nement of partial systems,*J. MSCS*, in press.
7. M. Sagiv, T. Reps, R. Wilhelm. Parametric Shape Analysis via 3-Valued Logic. 26th ACM POPL, 1999.
8. D.A. Schmidt. Binary Relations for Program Abstraction. In The Essence of Computation, Springer LNCS 2566, 2002.