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

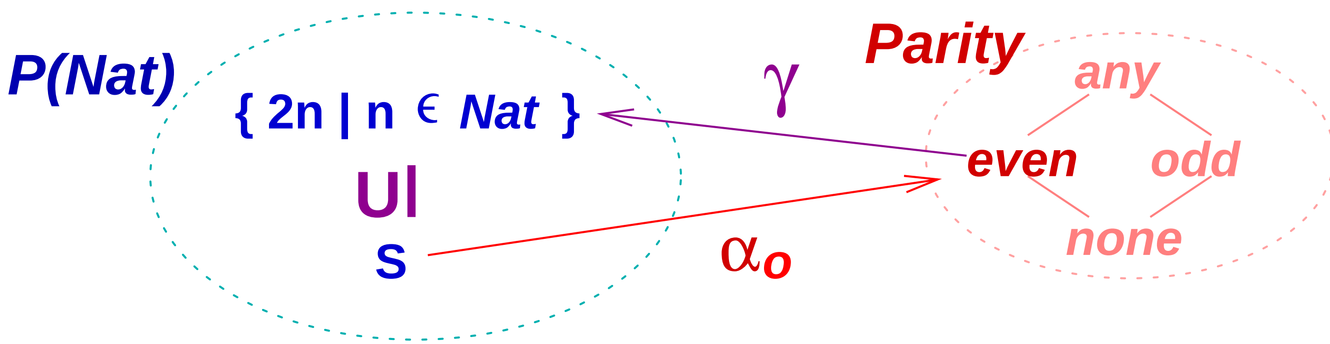
David Schmidt

Kansas State University and École Polytechnique

`www.cis.ksu.edu/~schmidt`

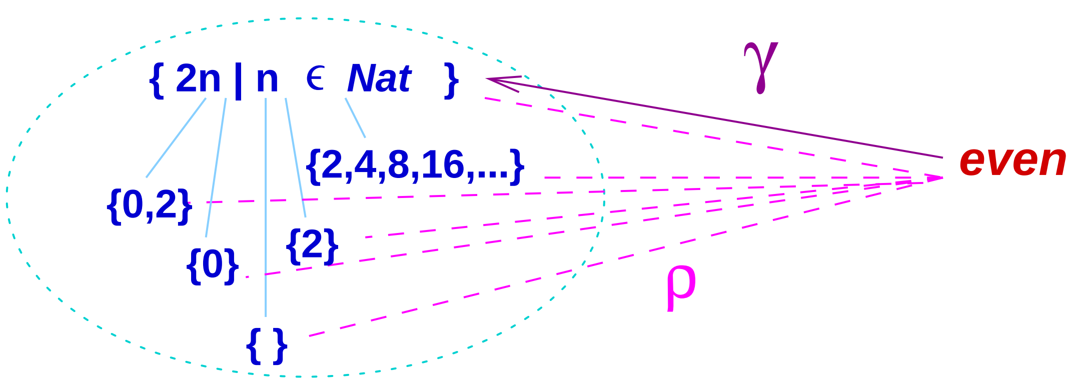
Background

Over-approximation *states a property of a program's outputs*



$even \in Parity$ asserts "$\forall even$" — all concrete outputs in set S are even-valued. (*We might write* $S \, \rho \, even$ *or* $S \models even$.)

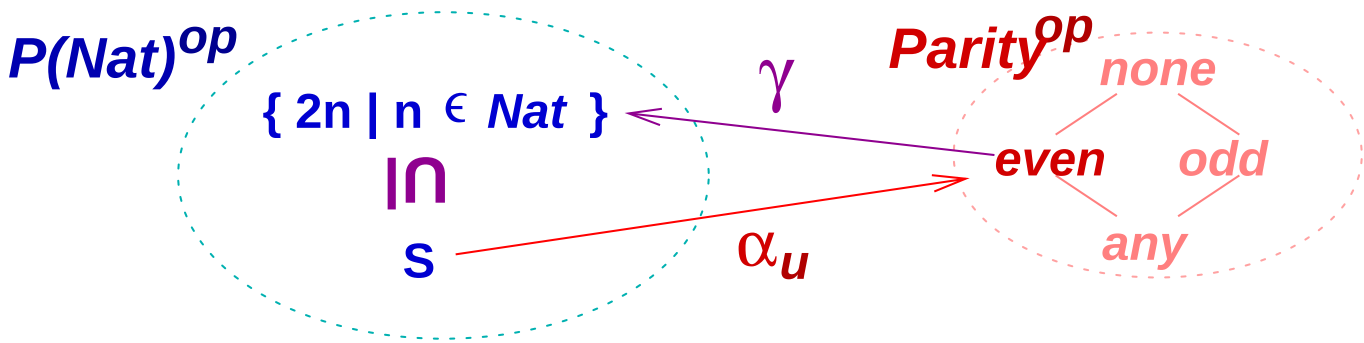
The upper adjoint, γ, selects the largest set approximated by $even$:



$$\gamma(a) = \cup\{S \mid S \, \rho \, a\}$$

Under-approximation *might be stated as the dual*

Here, $even$ assets that all evens are *included* in the concrete outputs:



This often abstracts constants to nothing, e.g., $[\![2]\!]^\flat_e = \mathrm{none}$, where $\gamma(\mathrm{none}) = \{\}$, because we require $\{2\} \supseteq \gamma(\alpha_u\{2\})$, forcing $\alpha_u\{2\} = \mathrm{none}$.

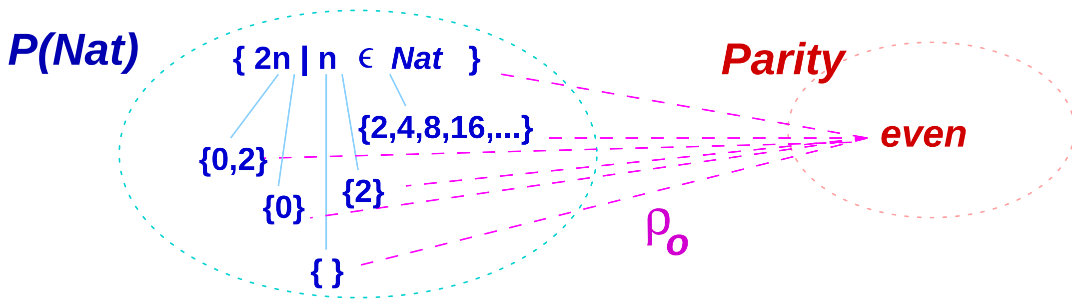
Thus, many program phrases are under-approximated to nothing:

$$[\![x+2]\!]^\flat_e = \mathrm{add}^\flat([\![x]\!]^\flat_e, [\![2]\!]^\flat_e) = \mathrm{add}^\flat(e(x), \mathrm{none}) = \mathrm{none}$$

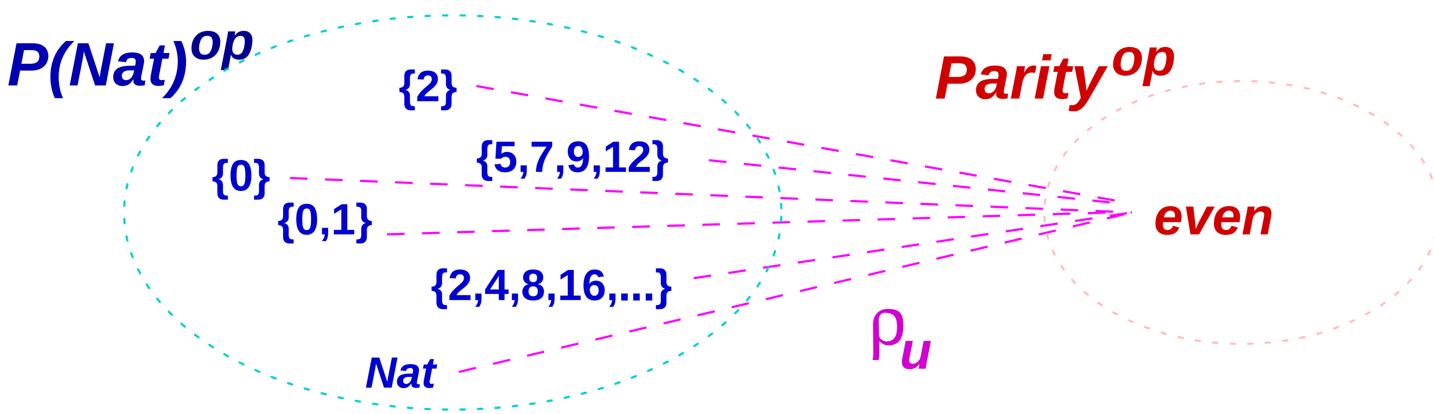
If we repair, say by including all constants, $n \in \mathrm{Nat}$, in $\mathrm{Parity}^{\mathrm{op}}$, then to preserve $\gamma(\sqcap_{\mathrm{Parity}^{\mathrm{op}}} W) = \cup_{a \in W}\, \gamma(a)$, we must expand $\mathrm{Parity}^{\mathrm{op}}$ into $\mathcal{P}(\mathrm{Nat})^{\mathrm{op}}$!

Under-approximation as existential quantification

If the over-approximating $even \in Parity$ asserts "$\forall even$,"

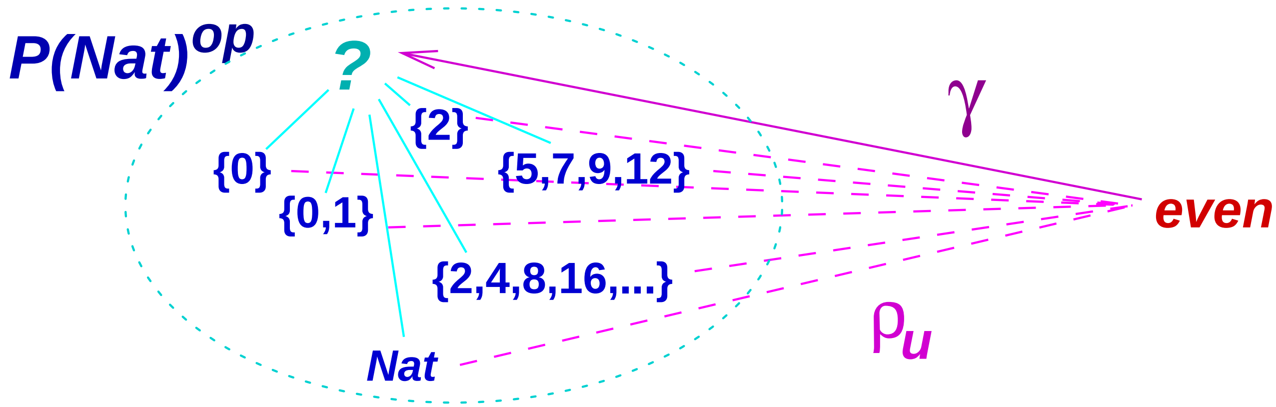


then the under-approximating $even \in Parity^{op}$ *should assert "*$\exists even$*"* — there exists an even number in the program's outputs:



This provides a nontrivial under-approximation of constants, e.g., $[\![2]\!]^\flat_e = even$, and expressions: $[\![x+2]\!]^\flat_e = add^\flat(e(x), even) = e(x)$.

But we cannot define $\gamma : \mathrm{Parity}^{op} \rightarrow \mathcal{P}(\mathrm{Nat})^{op}$ in the usual way:



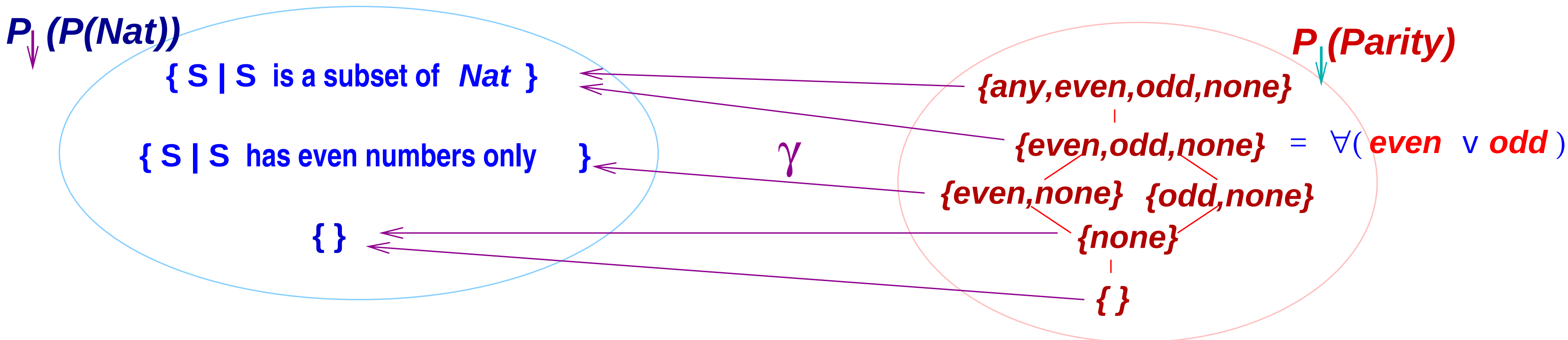
There is no best, minimal set that contains an even number.

Indeed, $even$'s concretization is not a single set — it is a *set of sets*:

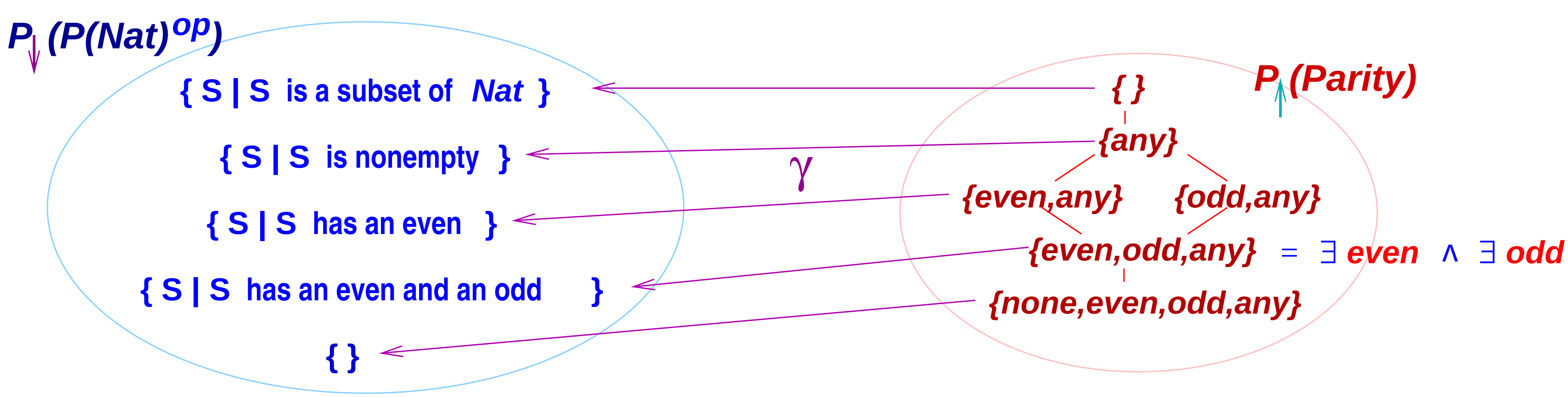
$$\gamma(even) = \{S \in \mathcal{P}(\mathrm{Nat})^{op} \mid S \; \rho_u \; even\}$$

This suggests that we work with *power-domains* in both the concrete and abstract domains.

Universal (over-approximating) interpretation: $\{even, odd\}$ asserts $\forall\{even, odd\} \equiv \forall(even \vee odd)$ — all outputs are even- or odd-valued: Use a lower power-domain (lower sets) for the abstract domain.



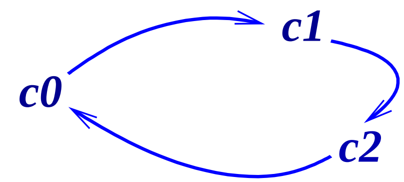
Existential (under-approximating) interpretation: $\{even, odd\}$ asserts $\exists\{even, odd\} \equiv \exists even \wedge \exists odd$ — there exists an even-valued and an odd-valued output: Use an upper power-domain (upper sets).



Dennis Dams's **mixed transition systems** *employ the universal and existential abstractions*

A transition system: $\Sigma = \{c_0, c_1, c_2\}$

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



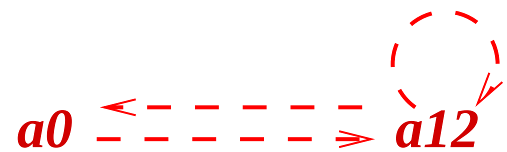
Approximating the states: Note: $\bot$ and $\top$ omitted for brevity.

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

That is, $c_0 \; \rho \; a_0$, $c_1 \; \rho \; a_{12}$, and $c_2 \; \rho \; a_{12}$.

Over-approximation transitions ("*may*"):

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



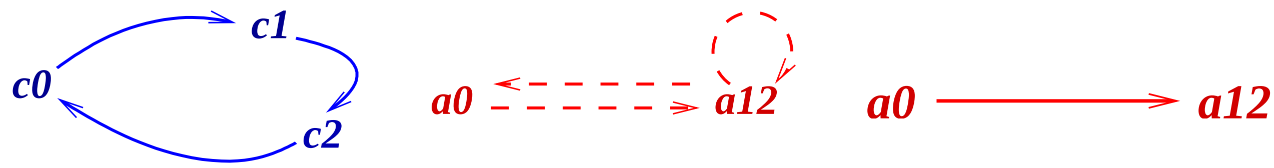
As a function, $R^\sharp(a_0) = \{a_{12}\} \equiv \forall a_{12}$ and $R^\sharp(a_{12}) = \{a_0, a_{12}\} \equiv \forall(a_0 \vee a_{12})$.

Under-approximation transitions ("*must*"):

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

As a function, $R^\flat(a_0) = \{a_{12}\} \equiv \exists a_{12}$ and $R^\flat(a_{12}) = \{\} \equiv \exists() \equiv \bot$

The *mixed transition system* is $(\{a_0, a_{12}\}, R^\flat, R^\sharp)$.



From Galois connection, $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$, Dams defines this *simulation relation*: $c\ \rho\ a$ *iff* $c \in \gamma(a)$. From $R \subseteq C \times C$, 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 $R \lhd_\rho R^\sharp$, that is, $R^\sharp$ ρ-*simulates* R
$R^\flat \lhd_{\rho^{-1}} R$, that is, $R^\flat$ *is* ρ-*simulated by* R

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

Define $a \models \Box\phi$ *iff for all* a', $aR^\sharp a'$ *implies* $a' \models \phi$
$a \models \Diamond\phi$ *iff there exists* a' *such that* $aR^\flat a'$ *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**: For all ρ-, ρ^{-1}-simulations of R, $R^\sharp$ and $R^\flat$ preserve the *most* $\Box\Diamond$-properties.

Can we derive $R^\sharp$ and $R^\flat$ and prove soundness and precision directly from Galois-connection theory?

Yes — we treat $R \subseteq C \times C$ as $R : C \to \mathcal{P}(C)$.

Then, we have $R^\sharp : A \to \mathcal{P}_L(A)$, where $\mathcal{P}_L(\cdot)$ is a *lower powerset* ($\subseteq$) constructor.

We "lift" the Galois connection, $\mathcal{P}(C)\langle\alpha_\tau, \gamma_\tau\rangle A$, on the states to a Galois connection on powersets, $F[\mathcal{P}(C)]\langle\alpha_{F[\tau]}, \gamma_{F[\tau]}\rangle\mathcal{P}_L(A)$, so that

1. $R^\sharp$ *ρ-simulates* R *iff* $\mathrm{ext}_{F[\tau]}(R) \circ \gamma_\tau \sqsubseteq_{A \to F[\mathcal{P}(C)]} \gamma_{F[\tau]} \circ R^\sharp$
2. *the soundness of* $a \models \Box\phi$ *follows from Item 1*
3. $R^\sharp{}_{best} = \alpha_{F[\tau]} \circ \mathrm{ext}_{F[\tau]}(R) \circ \gamma_\tau$

We do similar work for $R^\flat{}_{best} : A \to \mathcal{P}_U(A)$ and $\Diamond\phi$, where $\mathcal{P}_U(\cdot)$ is an *upper ($\supseteq$-ordered) powerset* constructor.

For over-approximation, we can use $F = \mathrm{id}$ or $F = \mathcal{P}_L(\cdot)$; for under-approximation, we must use $F = \mathcal{P}_L(\cdot^{op})$. (We will see why....)

Our results from reworking Dams's constructions

1. Starting from approximation relations, $\rho \subseteq C \times A$, we generate Galois connections from *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. They are the *join completions* of [*Cousot-Cousot ICCL 94*].

3. We use 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."

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 approximation relations

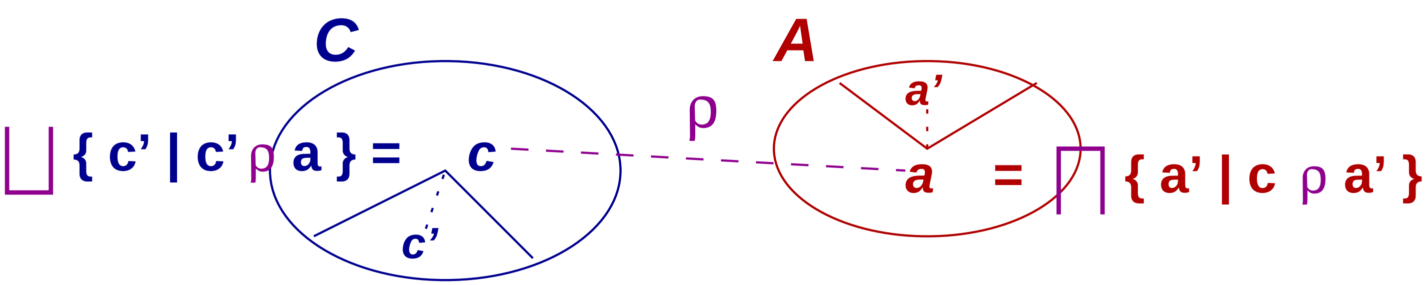
Closed relations and Galois connections

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

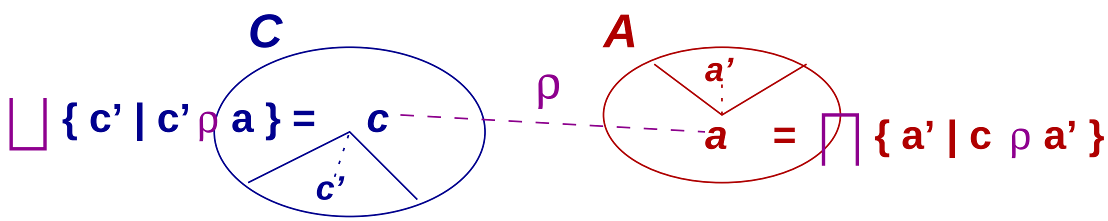
$c \; \rho \; a$ means that c is modelled/approximated by a

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-LUB-U-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 $\alpha_\rho c \sqsubseteq_A a$.

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,

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

“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.

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

Theorem: If ρ is U-GLB-closed, then $\bar{\rho}$ is L-LUB-U-GLB-closed, and $\mathcal{P}(C)\langle\alpha_{\bar{\rho}}, \gamma_{\bar{\rho}}\rangle A$ is a Galois connection, where $\gamma_{\bar{\rho}} a = \sqcup\{S \mid S\ \bar{\rho}\ a\} = \{c \mid c\ \rho\ a\}$.

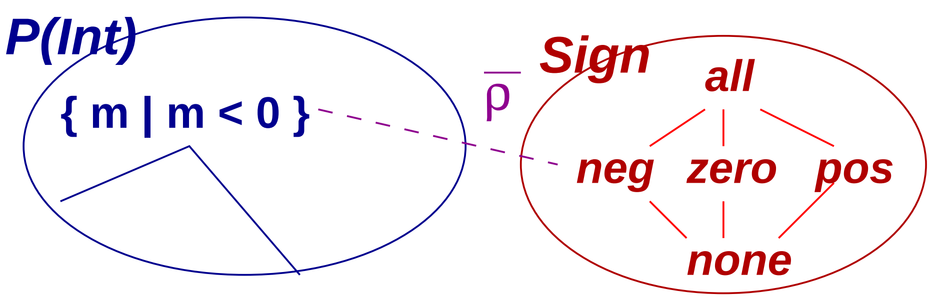
Example: Let Int be the discretely ordered set of integers:
$\rho \subseteq \mathrm{Int} \times \mathrm{Sign}$

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

$0\ \rho\ \mathrm{zero}$

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

$n\ \rho\ \mathrm{all}$



ρ is L-U-GLB-closed but not LUB-closed. It is completed to $\bar{\rho} \subseteq \mathcal{P}(\mathrm{Int}) \times \mathrm{Sign}$.

Powersets

Lower powersets

D's "powerset" is a complete lattice, E, with monotone *singleton* and *union* operations: $PD = (E, \sqsubseteq_E, \{\!|\cdot|\!\} : D \to E, \uplus : E \times E \to E)$.

Define *membership* as $c \tilde{\in} S$ iff $\{\!|c|\!\} \uplus S = S$.

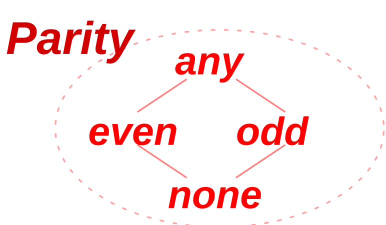
A *lower powerset*, $\mathcal{P}_L(D)$, treats $\sqsubseteq_E$ as $\subseteq$: For all $S_1, S_2 \in E$,

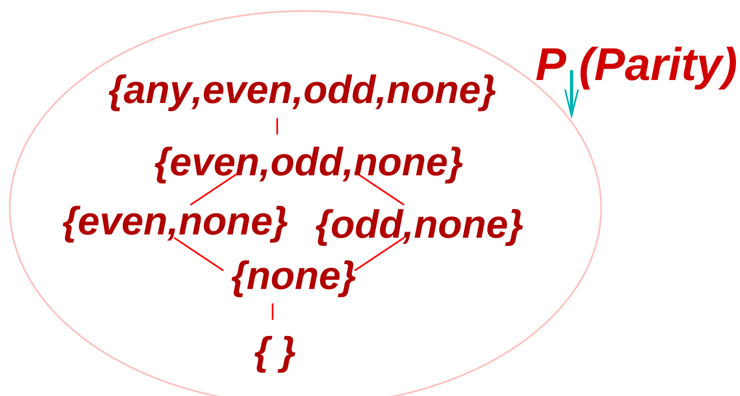
$S_1 \sqsubseteq_E S_2$ iff (for all $x \tilde{\in} S_1$, there exists $y \tilde{\in} S_2$ such that $x \sqsubseteq_D y$)

Down-set (order-ideal) completion: For $d \in D$, $S \subseteq D$, define $\downarrow d = \{e \in D \mid e \sqsubseteq_D d\}$ 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

Example:





Upper powersets

There is a dual construction:

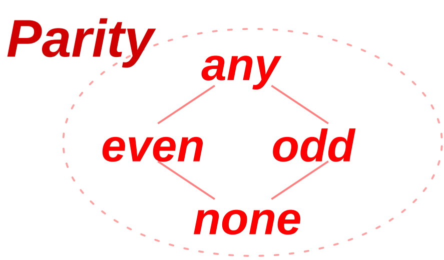
An *upper powerset*, $\mathcal{P}_u(D)$, treats $\sqsubseteq_E$ as $\supseteq$: For all $S_1, S_2 \in E$,

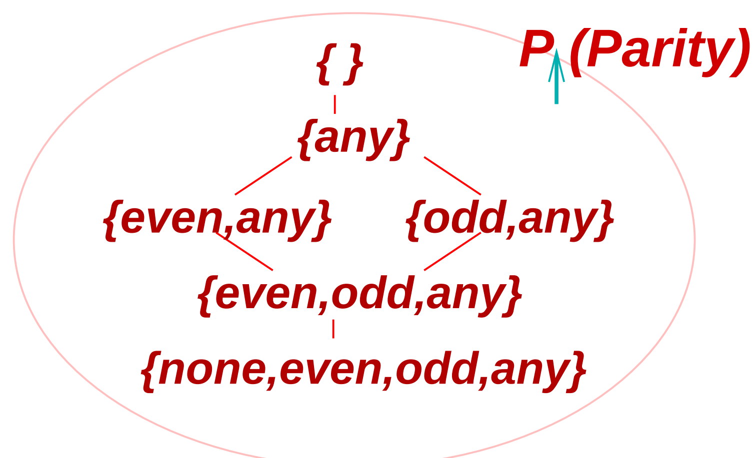
$S_1 \sqsubseteq_E S_2$ iff (for all $y \tilde{\in} S_2$, there exists $x \tilde{\in} S_1$ such that $x \sqsubseteq_D y$)

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

Example:





Logical relations

Logical relations

We now attach typings to the relations. Here are the types:

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

$\bar{\tau}$ is a special case of $\mathcal{P}_L(\tau)$ and names the completion of U-GLB-closed $\rho \subseteq C \times A$ to $\bar{\rho} \subseteq \mathcal{P}(C) \times A$, seen earlier

Let C_τ and A_τ be p.o.-sets of the appropriate form (e.g., $A_{\tau_1 \to \tau_2}$ is a lattice 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 $c \tilde{\in} S, c\ \rho_\tau\ a$. *That is,* $S\ \rho_{\bar{\tau}}\ a$ iff $S\ \rho_{\mathcal{P}_L(\tau)}\ \{\!|a|\!\}$

Simulation relations are 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, written $R \lhd_\rho R^\sharp$, iff for all $c, c' \in C$ and $a \in A$,
$c \, \rho \, a$ and $c \, R \, c'$ imply there exists $a' \in A$ s.t. $a \, R^\sharp \, a'$ and $c' \, \rho \, a'$.

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

Theorem:

1. $R \lhd_{\rho_b} R^\sharp$ iff $R \; \rho_{b \to \mathcal{P}_L(b)} \; R^\sharp$
2. $R^\flat \lhd_{\rho_b^{-1}} R$ iff $R \; \rho_{b \to \mathcal{P}_U(b)} \; R^\flat$

Closure properties of logical relations

$f\ \rho_{\tau_1 \to \tau_2}\ f^\sharp$ 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 $c \tilde{\in} S, c\ \rho_\tau\ a$

Theorem: For $\rho_\tau \subseteq C_\tau \times A_\tau$ 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 $\rho_{\mathcal{P}_U(\tau)}$.

Proposition: $\rho_{\bar{\tau}}$ and $\rho_{\mathcal{P}_L(\tau)}$ are always L-closed, and $\rho_{\mathcal{P}_U(\tau)}$ is always U-closed.

Alas, LUB-closure is not guaranteed for $\mathcal{P}_{\mathrm{L}}(\tau)$ and neither is GLB-closure for $\mathcal{P}_{\mathrm{U}}(\tau)$.

But there are some sufficient conditions upon the choice of lower- and upper-powerset that ensure these closures.

Here are two simple but useful examples:

Proposition: $\rho_{\mathcal{P}_{\mathrm{L}}(\tau)} \subseteq \mathcal{P}_{\downarrow}(C_\tau) \times \mathcal{P}_{\mathrm{L}}(A_\tau)$ is always LUB-closed.

Proposition: $\rho_{\mathcal{P}_{\mathrm{U}}(\tau)} \subseteq \mathcal{P}_{\mathrm{U}}(C_\tau) \times \mathcal{P}_{\uparrow}(A_\tau)$ is aways GLB-closed.

Dams's results

Synthesizing a most-precise simulation

Dams proved, for $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$ and transition relation $R \subseteq C \times C$, that the most-precise, sound abstract relation $R_0 \subseteq A \times A$ is

$$R_0(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in \min\{S' \mid R^{\exists\exists}(\gamma(a), S')\}\}$$

Reformatted as a function, this reads

$$R_0(a) = \{\alpha(s') \mid \exists s \in \gamma(a), s' \in R(s)\}$$

We can derive Dams's result: Given U-GLB-closed $\rho_b \subseteq C \times A$ and transition function $R : C \to \mathcal{P}(C)$, we derive $R_0 : A \to \mathcal{P}_\downarrow(A)$:

1. *We use the closure properties to generate L-LUB-U-GLB-closed relations,* $\rho_{\bar{b}} \subseteq \mathcal{P}(C) \times A$ *and* $\rho_{\mathcal{P}_L(b)} \subseteq \mathcal{P}(C) \times \mathcal{P}_\downarrow(A)$*.*
2. *We synthesize* $R^\sharp{}_{best} : A \to \mathcal{P}_\downarrow(A)$ *in the expected way:*

$$R^\sharp{}_{best} = \alpha_{\rho_{\mathcal{P}_L(b)}} \circ ext(R) \circ \gamma_{\rho_{\bar{b}}} = R_0$$

Synthesizing a most-precise **dual** *simulation*

Dams proved, for $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$ and $R \subseteq C \times C$, that the best underapproximating relation $R_1 \subseteq A \times A$ is

$$R_1(a, a') \text{ iff } a' \in \{\alpha(Y) \mid Y \in \min\{S' \mid R^{\forall\exists}(\gamma(a), S')\}\}$$

Reformatted as a function, this reads

$$R_1(a) = \{\alpha(Y) \mid Y \in \min\{S' \mid \text{for all } s \in \gamma(a), R(s) \cap S' \neq \{\}\}\}$$

We must work a bit harder, but we can derive the same result:

Given $R : C \to \mathcal{P}(C)$ and U-GLB-closed $\rho_b \subseteq C \times A$, we derive $R_1 : A \to \mathcal{P}_{\uparrow}(A)$....

We derive $R_1 : A \to \mathcal{P}_\uparrow(A)$:

1. *We generate L-LUB-U-GLB-closed* $\rho_{\bar{b}} \subseteq \mathcal{P}(C) \times A$
2. *We generate* $\rho_{\bar{\mathcal{P}}_U(b)} \subseteq \mathcal{P}_\downarrow(\mathcal{P}(C)^{op}) \times \mathcal{P}_\uparrow(A)$ *in stages:*
   (a) *begin with U-GLB-closed* $\rho_b \subseteq C \times A$ (because C is discretely ordered, ρ_b is L-closed also);
   (b) *lift to sets of answers*: lift the relation to L-U-GLB-closed $\rho_{\mathcal{P}_U(\tau)} \subseteq \mathcal{P}(C)^{op} \times \mathcal{P}_\uparrow(A)$;
   (c) *introduce LUB-closure (giving a Galois connection):* complete the relation to $\rho_{\bar{\mathcal{P}}_U(\tau)} \subseteq \mathcal{P}_\downarrow(\mathcal{P}(C)^{op}) \times \mathcal{P}_\uparrow(A)$.
3. *We synthesize* $R^\flat{}_{best} : A \to \mathcal{P}_\uparrow(A)$:

$$R^\flat{}_{best} = \alpha_{\rho_{\bar{\mathcal{P}}_U(b)}} \circ \mathit{ext}(\{\!|\cdot|\!\} \circ R) \circ \gamma_{\rho_{\bar{b}}} = R_1$$

where $\mathit{ext}(\{\!|\cdot|\!\} \circ R) : \mathcal{P}(C)^{op} \to \mathcal{P}_\downarrow(\mathcal{P}(C)^{op})$ maps a set of concrete arguments to the set of R-successor sets of the arguments.

As seen in the talk's introductory example, the relation in (b) lacks LUB-closure.

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 $S \in D_{\mathcal{P}_U(\tau)}$

The judgement form for $\bar{\tau}$ is a special case of $\mathcal{P}_L(\tau)$'s:

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

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

Some “syntactic sugar”:

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

$d \models \exists R\phi$ *(*$d \models \Diamond\phi$*)* 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 logic* or *description logic* or *branching-time temporal 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*.

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,

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

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

and prove these ρ_τ-sound as well.

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 $\models_{\tau}^{\neg pos} \phi$ 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}.

(i) 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.

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

(iii) 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.