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

David A. Schmidt[⋆]

Kansas State University, Manhattan, Kansas, USA, and
École Polytechnique, Palaiseau, FRANCE

Abstract. We redevelop and extend Dams's results on over- and under-approximation with higher-order Galois connections:
(1) We show how Galois connections are generated from U-GLB-L-LUB-closed binary relations, and we apply them to lower and upper powerset constructions, which are weaker forms of powerdomains appropriate for abstraction studies.
(2) We use the powerset types within a family of logical relations, show when the logical relations preserve U-GLB-L-LUB-closure, and show that simulation is a logical relation. We use the logical relations to rebuild Dams's most-precise simulations, revealing the inner structure of over- and under-approximation.
(3) We extract validation and refutation logics from the logical relations, state their resemblance to Hennessey-Milner logic and description logic, and obtain easy proofs of soundness and best precision.

Almost all Galois-connection-based static analyses are *over-approximating*: For Galois connection, $(\mathcal{P}(C), \subseteq)\langle\alpha_o, \gamma\rangle(A, \sqsubseteq_A)$, an abstract value $a \in A$ proclaims a property of all the outputs of a program. For example, $even \in Parity$ (see Figure 2 for the abstract domain *Parity*) asserts, "$\forall even$" — all the program's outputs are even numbers, that is, the output is a set from $\{S \in \mathcal{P}(Nat) \mid S \subseteq \gamma(even)\}$.

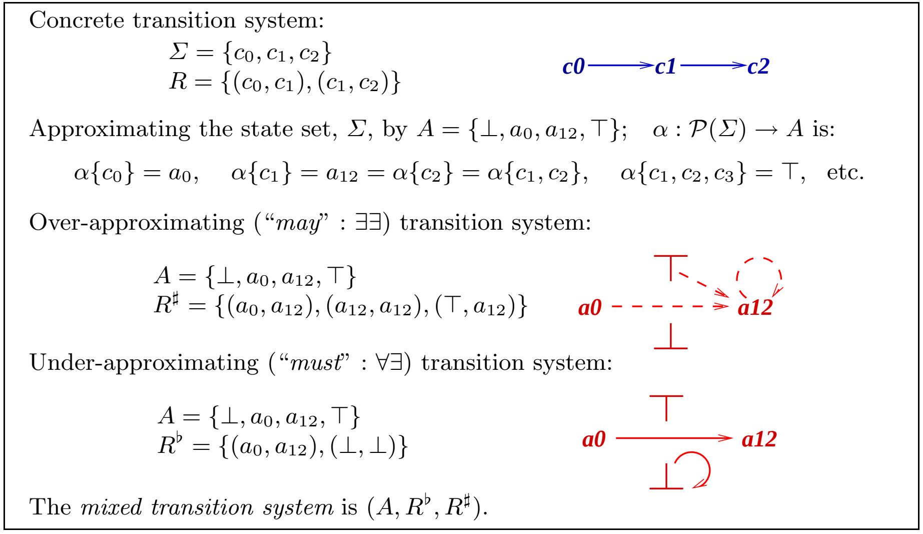
An *under-approximating* Galois connection, $(\mathcal{P}(C), \supseteq)\langle\alpha_u, \gamma\rangle A^{op}$, where $A^{op} = (A, \sqsupseteq_A)$, is the dual. Here, $even \in Parity^{op}$ asserts that *all even numbers are included in the program's outputs* — a strong assertion. Also, we may reuse $\gamma : A \to \mathcal{P}(C)$ as the upper adjoint from A^{op} to $\mathcal{P}(C)^{op}$ iff γ preserves joins in $(A, \sqsubseteq_A)$ — another strong demand.

Fortunately, there is an alternative view of under-approximation: $a \in A^{op}$ asserts an *existential property* — there exists an output with property a. For example, $even \in Parity^{op}$ asserts "$\exists even$" — there is an even number in the program's outputs, which is a set from $\{S \in \mathcal{P}(Nat) \mid S \cap \gamma(even) \neq \emptyset\}$.

Now, we can generalize both over- and under-approximation to multiple properties, e.g., $\forall\{even, odd\} \equiv \forall(even \vee odd)$ — all outputs are even- or odd-valued; and $\exists\{even, odd\} \equiv \exists even \wedge \exists odd$ — the output set includes an even value and an odd value. These examples "lift" A and A^{op} into the *powerset lattices*, $\mathcal{P}_L(A)$ and $\mathcal{P}_U(A)$, respectively, and set the stage for the problem studied in this paper.

[⋆] `schmidt@cis.ksu.edu`. Supported by NSF ITR-0085949 and ITR-0086154.

Fig. 1. An example mixed transition system



Concrete transition system:

$$\begin{aligned} \Sigma &= \{c_0, c_1, c_2\} \\ R &= \{(c_0, c_1), (c_1, c_2)\} \end{aligned}$$

Approximating the state set, Σ, by $A = \{\bot, a_0, a_{12}, \top\}$; $\alpha : \mathcal{P}(\Sigma) \to A$ is:

$$\alpha\{c_0\} = a_0, \quad \alpha\{c_1\} = a_{12} = \alpha\{c_2\} = \alpha\{c_1, c_2\}, \quad \alpha\{c_1, c_2, c_3\} = \top, \quad \text{etc.}$$

Over-approximating ("*may*" : ∃∃) transition system:

$$\begin{aligned} A &= \{\bot, a_0, a_{12}, \top\} \\ R^\sharp &= \{(a_0, a_{12}), (a_{12}, a_{12}), (\top, a_{12})\} \end{aligned}$$

Under-approximating ("*must*" : ∀∃) transition system:

$$\begin{aligned} A &= \{\bot, a_0, a_{12}, \top\} \\ R^\flat &= \{(a_0, a_{12}), (\bot, \bot)\} \end{aligned}$$

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

1 Dams's mixed-transition systems

In his thesis [10] and in subsequent work [11], Dams studied over- and under-approximations of state-transition relations, $R \subseteq C \times C$, for a discretely ordered set, C, of states. Given complete lattice $(A, \sqsubseteq_A)$ and the Galois connection, $(\mathcal{P}(C), \subseteq)\langle\alpha, \gamma\rangle(A, \sqsubseteq_A)$, Dams defined an over-approximating transition relation, $R^\sharp \subseteq A \times A$, and an *under-approximating* transition relation, $R^\flat \subseteq A \times A$, as follows:

$$\begin{aligned} aR^\sharp a' &\text{ iff } a' \in \{\alpha(Y) \mid Y \in min\{S' \mid R^{\exists\exists}(\gamma(a), S')\}\} \\ aR^\flat a' &\text{ iff } a' \in \{\alpha(Y) \mid Y \in min\{S' \mid R^{\forall\exists}(\gamma(a), S')\}\}^1 \end{aligned}$$

such that $R^\sharp$ *ρ-simulates* R (that is, all R-transitions are mimicked by $R^\sharp$, modulo $\rho \subseteq C \times A$, where $c\,\rho\,a$ *iff* $c \in \gamma(a)$), and R ρ^{-1}*-simulates* $R^\flat$. See Figure 1 for an example of R and its *mixed transition system*, $R^\flat$, $R^\sharp$.

For the branching-time modalities $\Box$ $(\forall R)$ and $\Diamond$ $(\exists R)$,

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

Dams proved soundness: $a \models \phi$ *and* $c\,\rho\,a$ *imply* $c \models \phi$. With impressive work, Dams also proved "best precision" [11]: For all ρ- (and ρ^{-1}-) simulations, $R^\sharp$ and $R^\flat$ preserve the most $\Box\Diamond$-(*mu-calculus* [20, 21]) properties.

[1] $R^{\exists\exists}$, $R^{\forall\exists}$, and the definitions themselves are explained later in the paper.

1.1 Can we derive Dams's results within Galois-connection theory?

Given that Dams begins with a Galois connection, it should be possible to reconstruct his results entirely within a theory of higher-order Galois connections and gain new insights in the process. We do so in this paper.

First, we treat $R \subseteq C \times C$ as $R : C \rightarrow \mathcal{P}(C)$. This makes $R^\sharp : A \rightarrow \mathcal{P}_L(A)$, where $\mathcal{P}_L(\cdot)$ is a *lower ($\subseteq$-ordered) powerset* constructor.[2]

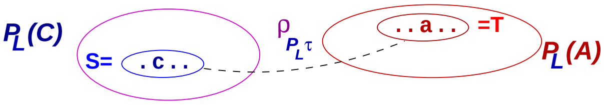
Given the Galois connection, $\mathcal{P}(C)\langle\alpha_\tau, \gamma_\tau\rangle A$, on states, we "lift" it to a Galois connection on powersets, $F[\mathcal{P}(C)]\langle\alpha_{F[\tau]}, \gamma_{F[\tau]}\rangle\mathcal{P}_L(A)$, so that

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

We do similar work for $R^\flat_{best} : A \rightarrow \mathcal{P}_U(A)$ and $\Diamond\phi$, where $\mathcal{P}_U(\cdot)$ is an *upper ($\supseteq$-ordered) powerset* constructor.[3]

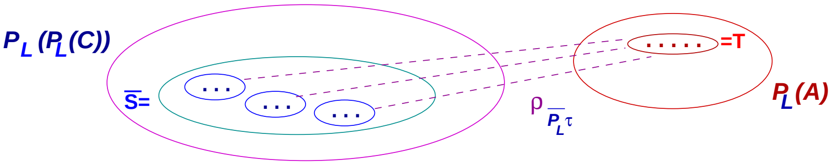
The crucial question is: *What is $F[\mathcal{P}(C)]$*? That is, *how should we concretize a set $T \in \mathcal{P}_L(A)$?* First, we write $c \, \rho_\tau \, a$ to assert that $c \in C$ is approximated by $a \in A$. (For example, for Galois connection, $\mathcal{P}(C)\langle\alpha_\tau, \gamma_\tau\rangle A$, define $c \, \rho_\tau \, a$ iff $c \in \gamma_\tau(a)$.) Then, $S \in \mathcal{P}(C)$ is approximated by $T \in \mathcal{P}_L(A)$ iff $S \, \rho_{\mathcal{P}_L(\tau)} \, T$, where

$$S \, \rho_{\mathcal{P}_L(\tau)} \, T \text{ iff for every } c \in S, \text{ there exists } a \in T \text{ such that } c \, \rho_\tau \, a$$ [4]



This might suggest that $F[\mathcal{P}(C)]$ is just $\mathcal{P}(C)$, and the concretization, $\gamma_{\mathcal{P}(\rho_\tau)} : \mathcal{P}_L(A) \rightarrow \mathcal{P}(C)$, is $\gamma_{\mathcal{P}(\rho_\tau)}(T) = \cup\{S \mid S \, \rho_{\mathcal{P}_L(\tau)} \, T\}$, which concretizes T to the largest set that is approximated by T.

But, as suggested by this paper's prelude, an alternative is to define $F[\mathcal{P}(C)]$ as $\mathcal{P}_L(\mathcal{P}(C))$, because if an abstract state $a \in A$ concretizes to a *set of states*, $\gamma_\tau(a) \subseteq C$, then set $T \in \mathcal{P}_L(A)$ should concretize to a *set of sets of states*:



That is, $\bar{S} \in \mathcal{P}_L(\mathcal{P}(C))$ is approximated by $T \in \mathcal{P}_L(A_\tau)$ iff for every set $S \in \bar{S}$, $S \, \rho_{\mathcal{P}_L(\tau)} \, T$. This makes $\gamma_{\bar{\mathcal{P}}_L(\tau)}(T) = \{S \mid S \, \rho_{\mathcal{P}_L(\tau)} \, T\}$, which concretizes T to the set of all sets approximated by T.

For over-approximation, both approaches yield the *same* definition of $R^\sharp_{best} : A \rightarrow \mathcal{P}_L(A)$, but a sound under-approximation *utilizes the second approach*:

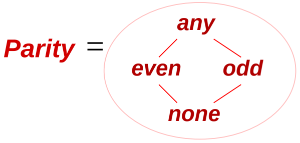
[2] Think of the elements of $\mathcal{P}_L(A)$ as sets of properties, like $\forall\{\mathit{even}, \mathit{odd}\}$, as described in the prelude to Section 1.

[3] Think of the elements of $\mathcal{P}_U(A)$ as sets of properties, like $\exists\{\mathit{even}, \mathit{odd}\}$.

[4] This is the lower half of the Egli-Milner ordering, such that when $\rho_\tau \subseteq C \times C$ equals $\sqsubseteq_\tau$, freely generates the lower ("Hoare") powerdomain.

Fig. 2. An under-approximation of sets of natural numbers by sets of parities

Let Nat be the discretely ordered set of natural numbers,
and let complete lattice

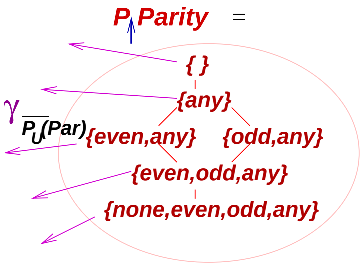


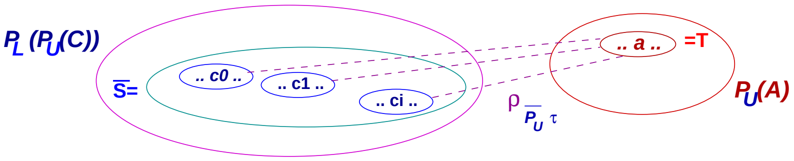
We have the obvious Galois connection, $\mathcal{P}(Nat)\langle\alpha_{Par}, \gamma_{Par}\rangle Parity$, where $\gamma_{Par}(even) = \{2n \mid n \in Nat\}$, $\gamma_{Par}(any) = Nat$, etc. We can lift this to:

$$\gamma_{\bar{\mathcal{P}}_U(Par)} : \mathcal{P}_\uparrow(Parity) \rightarrow \mathcal{P}_\downarrow(\mathcal{P}(Nat)^{op})$$

where $\mathcal{P}_\uparrow(Parity)$ are the superset-ordered, up-closed subsets of $Parity$, and $\mathcal{P}_\downarrow(\mathcal{P}(Nat)^{op})$ are the subset-ordered, superset-closed subsets of $\mathcal{P}(Nat)$. $\gamma_{\bar{\mathcal{P}}_U(Par)}$ is defined as follows:

$\gamma_{\bar{\mathcal{P}}_U(Par)}\{\} =$ all subsets of Nat
$\supseteq$
$\gamma_{\bar{\mathcal{P}}_U(Par)}\{any\} =$ nonempty subsets of Nat
$\supseteq$
$\gamma_{\bar{\mathcal{P}}_U(Par)}\{even, any\} =$ all sets with
an even number $\supseteq$
$\gamma_{\bar{\mathcal{P}}_U(Par)}\{even, odd, any\} =$ all sets with
an even and an odd number $\supseteq$
$\gamma_{\bar{\mathcal{P}}_U(Par)}\{none, even, odd, any\} = \{\}$





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

$S\, \rho_{\mathcal{P}_U(\tau)}\, T$ *iff for every* $a \in T$*, there exists some* $c \in S$ *such that* $c\, \rho_\tau\, a$.[5]

Thus, $\gamma_{\bar{\mathcal{P}}_U(\tau)} : \mathcal{P}_U(A) \rightarrow \mathcal{P}_L(\mathcal{P}(C)^{op})$, and $\gamma_{\bar{\mathcal{P}}_U(\tau)}(T) = \{S \mid S\, \rho_{\mathcal{P}_U(\tau)}\, T\}$, which is crucial to Dams's results. Figure 2 gives an example of the construction.

1.2 Outline of Results

Applying the just-stated approach, we redevelop and extend Dams's results [10, 11] within a higher-order Galois-connection framework [9]:

[5] This is the upper half of the Egli-Milner ordering, and when $\rho_\tau \subseteq C \times C$ is $\sqsubseteq_\tau$, freely generates the upper ("Smyth") powerdomain.

1. We show how Galois connections are generated from U-GLB-L-LUB-closed binary relations (cf. [8, 23, 28]).
2. We define lower and upper powerset constructions, which are weaker forms of powerdomains appropriate for abstraction studies [9, 15, 25].
3. We use the powerset types within a family of logical relations, show when the logical relations preserve the closure properties in Item 1., and show that simulation can be proved via logical relations. We incrementally rebuild Dams's most-precise simulations with the logical relations, revealing the inner structure of under- and over-approximation on powersets.
4. We extract validation and refutation logics from the logical relations (cf. [2]), state their resemblance to Hennessey-Milner logic [17] and description logic [3, 6], and obtain easy proofs of soundness and best precision.

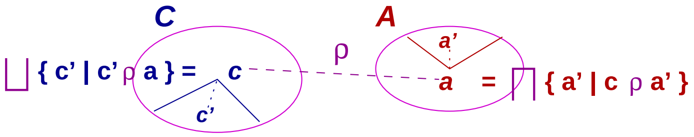
2 Closed binary relations generate Galois connections

The following results are assembled from [4, 8, 14, 23, 24, 28]: Let C and A be complete lattices, and let $\rho \subseteq C \times A$, where $c\,\rho\,a$ means c is approximated by a.

Definition 1. *For all $c, c' \in C$, for $a, a' \in A$, for $\rho \subseteq C \times A$, ρ is*

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

Proposition 2. *For L-U-LUB-GLB-closed $\rho \subseteq C \times A$, $C\langle\alpha_\rho, \gamma_\rho\rangle A$ is a Galois connection, where $\alpha_\rho(c) = \sqcap\{a \mid c\,\rho\,a\}$ and $\gamma_\rho(a) = \sqcup\{c \mid c\,\rho\,a\}$.*



As the diagram above suggests, U- and L-closure make γ_ρ and α_ρ monotonic, and LUB- and GLB- closure make the functions select the most precise answers. Note that $c\,\rho\,a$ iff $c \sqsubseteq_C \gamma_\rho(a)$ iff $\alpha_\rho(c) \sqsubseteq_A a$.

Proposition 3. *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, $\rho_{\alpha\gamma}$ is L-U-LUB-GLB-closed and $\langle\alpha_{\rho_{\alpha\gamma}}, \gamma_{\rho_{\alpha\gamma}}\rangle = \langle\alpha, \gamma\rangle$.*

2.1 Completing a U-GLB-closed $\rho \subseteq C \times A$

Often one has a discretely ordered set, C, a complete lattice, A, and an obvious approximation relation, $\rho \subseteq C \times A$. But there is no Galois connection between C and A, because ρ lacks LUB-closure. We complete C to a powerset:

Proposition 4. *For set C, complete lattice A, and $\rho \subseteq C \times A$, define $\bar{\rho} \subseteq \mathcal{P}(C) \times A$ as $S\,\bar{\rho}\,a$* iff for all $c \in S$, $c\,\rho\,a$. *If ρ is U-GLB-closed, then $\bar{\rho}$ is U-GLB-L-LUB-closed and $\gamma_{\bar{\rho}} : A \to \mathcal{P}(C)$ is $\gamma_{\bar{\rho}}(a) = \{c \mid c\,\rho\,a\}$.*

Figure 3 shows an application. There is no implementation penalty in applying Proposition 4, because the abstract domain retains its existing cardinality.

Fig. 3. Completing $\rho \subseteq \mathit{Int} \times \mathit{Sign}$ to $\bar{\rho} \subseteq \mathcal{P}(\mathit{Int}) \times \mathit{Sign}$

$\rho \subseteq \mathit{Int} \times \mathit{Sign}$
$n\, \rho\, \mathit{neg}$, for $n < 0$
$0\, \rho\, \mathit{zero}$
$p\, \rho\, \mathit{pos}$, for $p > 0$
$i\, \rho\, \mathit{any}$, for $i \in \mathit{Int}$

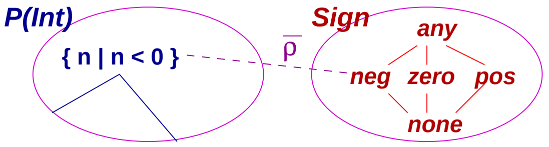
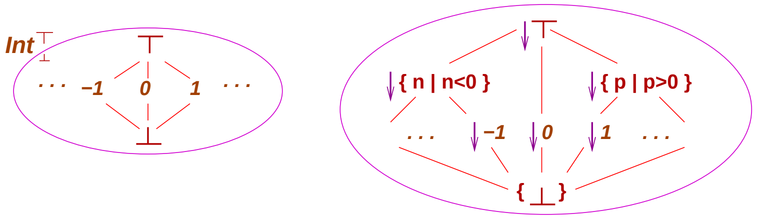


Fig. 4. Complete lattice $\mathit{Int}_{\perp}^{\top}$ and one possible join completion



3 Powersets

Definition 5. *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*
- $\{\!|\cdot|\!\}$, *the singleton operation, is monotone*
- $\uplus$, *union operation, is monotone, absorptive, commutative, and associative*
- *For every monotone $f : D \to L$, there is a monotone $\mathit{ext}(f) : E \to L$ such that $\mathit{ext}(f)\{\!|d|\!\} = f(d)$, for all $d \in D$.*

Here are examples of powersets from Cousot and Cousot [9]:
Down-set (order-ideal) completion: 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 $\mathcal{P}_{\downarrow}(D) = (\{\downarrow S \mid S \subseteq D\}, \subseteq, \downarrow, \cup)$.
Join completion (subsets 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* (that is, closed under intersections). [6]

Figure 4 presents an example. For monotone $f : D \to L$, let $\mathit{ext}(f) : \mathcal{P}_{\downarrow}(D) \to L$ be $\mathit{ext}(f)(S) = \sqcup_{d \in S} f(d)$.
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 $\mathcal{P}_{\uparrow}(D) = (\{\uparrow S \mid S \subseteq D\}, \supseteq, \uparrow, \cup)$.
Dual-join completion: subsets of $\mathcal{P}_{\uparrow}(D)$: $(\mathcal{M}, \supseteq, \uparrow, \sqcap_{\mathcal{M}})$, where $\mathcal{M} \subseteq \{\uparrow S \mid S \subseteq D\}$ is a Moore family.

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

[6] Join completions "add new joins" to D; the trivial join completion is $(\{\downarrow d \mid d \in D\}, \subseteq, \downarrow, \downarrow \circ \sqcup_D)$, which is isomorphic to D, and the most detailed join completion is $\mathcal{P}_{\downarrow}(D)$.

3.1 Lower and strongly lower powersets

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

Definition 6. *Powerset* $\mathcal{P}_L(D) = (E, \sqsubseteq_E, \{\!| \cdot |\!\}, \uplus)$ *is*

1. *a* lower powerset *iff ((for all* $x \tilde{\in} S_1$*, there exists* $y \tilde{\in} S_2$ *such that* $x \sqsubseteq_D y$*) implies* $S_1 \sqsubseteq_E S_2$*).*
2. *a* strongly *lower powerset iff ((for all* $x \tilde{\in} S_1$*, there exists* $y \tilde{\in} S_2$ *such that* $x \sqsubseteq_D y$*) iff* $S_1 \sqsubseteq_E S_2$*).*

Although lower powersets are the starting point for powerdomain theory [15, 25][7], we work with strongly lower powersets[8], because

Proposition 7. *For every strongly lower powerset,* $\mathcal{P}_L(D) = (E, \sqsubseteq_E, \{\!| \cdot |\!\}, \uplus)$*,*
(i) $\uplus = \sqcup_E$*; and*
(ii) $\mathcal{P}_L(D)$ *is order-isomorphic to a join-completion of* D*, where* $\tilde{\in}$ *is* $\in$*.*

Strongly lower powersets let us generalize Proposition 4:

Theorem 8. *For complete lattices* C *and* A*, let* $\rho \subseteq C \times A$ *and let* $\mathcal{P}_L(C) = (E, \subseteq, \{\!| \cdot |\!\}, \uplus)$ *be a join completion (strongly lower powerset). Recall that* $\bar{\rho} \subseteq \mathcal{P}_L(C) \times A$ *is defined* $S\, \bar{\rho}\, a$ iff for all $c \in S$, $c\, \rho\, a$.

If (i) ρ *is U-L-GLB-closed, and* (ii) *for all* $a \in A$*,* $\{c \mid c\, \rho\, a\} \in E$*,* then $\bar{\rho}$ *is U-L-GLB-LUB-closed and* $\gamma_{\bar{\rho}}(a) = \{c \mid c\, \rho\, a\}$*.*

Thus, $\mathcal{P}_{\downarrow}(C)\langle \alpha_{\bar{\rho}}, \gamma_{\bar{\rho}} \rangle A$ is always a Galois connection for U-L-GLB-closed $\rho \subseteq C \times A$, but the *minimal* join completion of sets $\{c \mid c\, \rho\, a\}$, $a \in A$, also suffices to generate a Galois connection.

For example, say that *Int* and ρ in Figure 3 are replaced by $Int_{\perp}^{\top}$ from Figure 4 and by $\rho \subseteq Int_{\perp}^{\top} \times Sign$, which is defined to be ρ augmented by $\top\, \rho\, any$ and $\perp\, \rho\, a$, for all $a \in Sign$. Figure 4 shows ρ's minimal join completion.

3.2 Upper powersets

As Plotkin [25] notes, the upper and strongly upper powersets coincide, so

Definition 9. *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* $x \sqsubseteq_\tau y$*).*

For an upper powerset, $\uplus = \sqcap$, and every upper powerset is isomorphic to a dual-join completion.

[7] which requires functions to be Scott-continuous

[8] which allows non-Scott-continuous, monotone functions

4 Logical relations

We attach these typings to the relations introduced in Section 2:

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

Only typing $\bar{\tau}$ is nonstandard; it is a special case of $\mathcal{P}_L(\tau)$ that we retain for convenience, because it appears so often in the practice of generating Galois connections.

We attach the typings to concrete and abstract domains, D, as follows:

D_b is given, for base type b
$D_{\tau_1 \to \tau_2}$ are the monotone functions from D_{τ_1} to D_{τ_2}, ordered pointwise
$D_{\mathcal{P}_L(\tau)}$ is a strongly lower powerset generated from D_τ
$D_{\mathcal{P}_U(\tau)}$ is an upper powerset generated from D_τ

Since $\bar{\rho} \subseteq \mathcal{P}_L(C) \times A$ is the completion of $\rho \subseteq C \times A$ (cf. Theorem 8), we define

$$C_{\bar{\tau}} \text{ is } C_{\mathcal{P}_L(\tau)}, \text{ for concrete domain } C_\tau$$
$$A_{\bar{\tau}} \text{ is } A_\tau, \text{ for abstract domain } A_\tau$$

Now, we can define this family of logical relations, $\rho_\tau \subseteq C_\tau \times A_\tau$:

ρ_b is given, for base type b
$f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp$ 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 $c \in S, c \, \rho_\tau \, a$

Again, note that $\rho_{\bar{\tau}} \subseteq C_{\mathcal{P}_L(\tau)} \times A_\tau$ is an instance of $\rho_{\mathcal{P}_L(\tau)} \subseteq C_{\mathcal{P}_L(\tau)} \times A_{\mathcal{P}_L(\tau)}$, where $C_{\mathcal{P}_L(\tau)}$ is treated as a join completion and $A_{\mathcal{P}_L(\tau)}$ is restricted to the trivial join completion, $(\{\downarrow a \mid a \in A_\tau\}, \subseteq, \downarrow, \downarrow \circ \sqcup_{A_\tau})$, which is isomorphic to A_τ.

4.1 Simulations are logical relations

The standard definition of simulation goes as follows:

Definition 10. *For $\rho \subseteq C \times A$ and transition relations, $R \subseteq C \times C$, $R^\sharp \subseteq A \times A$, $R^\sharp$ ρ-simulates R, written $R \lhd_\rho R^\sharp$, iff for all $c, c' \in C, a \in A$,*

$$c \, \rho \, a \textit{ and } c \, R \, c' \textit{ imply there exists } a' \in A \textit{ such that } a \, R^\sharp \, a' \textit{ and } c' \, \rho \, a'.$$

When we represent R and $R^\sharp$ as $R : C \to \mathcal{P}_L(C)$ and $R^\sharp : A \to \mathcal{P}_L(A)$, respectively, we have

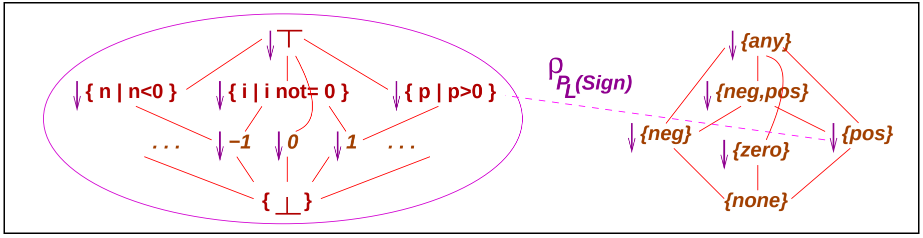
Theorem 11. $R \lhd_{\rho_b} R^\sharp$ *iff* $R \, \rho_{b \to \mathcal{P}_L(b)} \, R^\sharp$. [9]

A dual simulation, $R^\flat \lhd_{\rho_b^{-1}} R$, is beautifully characterized as $R \, \rho_{b \to \mathcal{P}_U(b)} \, R^\flat$. We employ these characterizations of simulation and dual-simulation to construct optimal over- and under-approximating transition relations from Galois connections generated from closed, logical relations. [10]

[9] The proof assumes that R and $R^\sharp$ behave monotonically.

[10] Please see Section 8 for a summary of Loiseaux, et al. [22], which also characterizes simulations as Galois connections.

Fig. 5. An L-LUB-closed relation between strongly lower powersets



5 Closure properties of logical relations

Proposition 12. *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 $\rho_{\mathcal{P}_U(\tau)}$.

Preservation of LUB-closure for $\rho_{\mathcal{P}_L(\tau)}$ and GLB-closure for $\rho_{\mathcal{P}_U(\tau)}$ depend on the specific powersets used (cf. Backhouse and Backhouse [4]).

Here are some additional useful properties:

Proposition 13. *Let $\rho_{\tau_i} \subseteq C_{\tau_i} \times A_{\tau_i}$, for $i \in 1..2$, be U-GLB-L-LUB-closed. For $f : C_{\tau_1} \to C_{\tau_2}$, $f^\sharp : A_{\tau_1} \to A_{\tau_2}$,*

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

In particular, $f \, \rho_{\tau_1 \to \tau_2} \, f^\sharp{}_{best}$, where $f^\sharp{}_{best}(a) = \alpha_{\rho_{\tau_2}} \circ f \circ \gamma_{\rho_{\tau_1}}$.

If $\rho_\tau \subseteq C_\tau \times A_\tau$ is L-LUB-closed, *then so is $\rho_{\mathcal{P}_L(\tau)} \subseteq \mathcal{P}_\downarrow(C_\tau) \times \mathcal{P}_L(A_\tau)$, for any choice of $\mathcal{P}_L(A_\tau)$*; this follows from

Proposition 14. *For all $T \in \mathcal{P}_L(A_\tau)$, let $\mathcal{L}_T = \{S \in \mathcal{P}_L(C_\tau) \mid S \, \rho_{\mathcal{P}_L(\tau)} \, T\}$. If*

1. *ρ_τ is L-LUB-closed; and*
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 $\rho_{\mathcal{P}_L(\tau)} \subseteq \mathcal{P}_L(C_\tau) \times \mathcal{P}_L(A_\tau)$ is LUB-closed.

That is, given the lower powerset $\mathcal{P}_L(C_\tau)$, we require $\sqcup \mathcal{L}_T \, \rho_{\mathcal{P}_L(\tau)} \, T$, for all $T \tilde{\in} A_{\mathcal{P}_L(\tau)}$. Item *2* says that every element, $c \tilde{\in} \sqcup \mathcal{L}_T$, is a join of elements that are all related to some $a \tilde{\in} T$. By L-LUB closure of ρ_τ, we have $c \, \rho_\tau \, a$, giving LUB-closure for $\rho_{\mathcal{P}_L(\tau)}$.

Often we can use a coarser join completion than $\mathcal{P}_\downarrow(C_\tau)$ to get LUB-closure. For example, for $C_{Int} = Int_\bot^\top$ from Figure 4 and $A_{Int} = Sign$ from Figure 3, the version of $\mathcal{P}_L(Sign)$ in Figure 5(*right*), requires merely the $\mathcal{P}_L(Int_\bot^\top)$ in Figure 5(*left*), for LUB-closure of $\rho_{\mathcal{P}_L(Sign)} \subseteq \mathcal{P}_L(Int_\bot^\top) \times \mathcal{P}_L(Sign)$.[11]

[11] Of course, for $\mathcal{P}_L(C_\tau)$ to be useful for giving the semantics of transition relation $R \subseteq C_\tau \times C_\tau$, we require that $\downarrow\{c' \mid cRc'\} \in \mathcal{P}_L(C_\tau)$, for all $c \in C_\tau$.

Proposition 15. *For all $S \in \mathcal{P}_U(C_\tau)$, 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, and*
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 $\rho_{\mathcal{P}_U(\tau)} \subseteq \mathcal{P}_U(C_\tau) \times \mathcal{P}_U(rA_\tau)$ is GLB-closed.

For all choices of $\mathcal{P}_U(C_\tau)$, Proposition 15 successfully applies to $\mathcal{P}_\uparrow(A_\tau)$, the filter completion of A_τ. But often a coarser, dual-join completion of A_τ will do: When giving semantics to transition relation $R \subseteq C_\tau \times C_\tau$, we require only that R's image lies in $\mathcal{P}_U(C_\tau)$: $\uparrow\{c' \mid cRc'\} \in \mathcal{P}_U(C_\tau)$, for all $c \in C_\tau$. This coarser domain for $\mathcal{P}_U(C_\tau)$ lets us use a coarser $\mathcal{P}_U(A_\tau)$ with Proposition 15.

6 Synthesizing a most-precise simulation

Dams [10, 11] proves, for Galois connection $\mathcal{P}(C)\langle\alpha,\gamma\rangle A$ and relation $R \subseteq C \times C$, that the most precise, sound, abstract transition relation $R_0^\sharp \subseteq A \times A$ is

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

where $R^{\exists\exists}(M,N)$ *holds iff there exist $m \in M$ and $n \in N$ such that mRn.* Recoded as a function, $R_0^\sharp : A \to \mathcal{P}_L(A)$, and simplified, this reads

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

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 the Galois connections, $\mathcal{P}(C)\langle\alpha_{\rho_{\bar{b}}},\gamma_{\rho_{\bar{b}}}\rangle A$ and $\mathcal{P}(C)\langle\alpha_{\rho_{\mathcal{P}_L(b)}},\gamma_{\rho_{\mathcal{P}_L(b)}}\rangle\mathcal{P}_L(A)$, and synthesize the most precise, sound abstract transition function, $R^\sharp_{best} : A \to \mathcal{P}_L(A)$,

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

which is Dams's definition, when $\mathcal{P}_L(A)$ is $\mathcal{P}_\downarrow(A)$. We have $R\,\rho_{\bar{b}\to\mathcal{P}_L(b)}\,R^\sharp_{best}$.

As suggested in Section 1.1, we might also derive an abstract transition relation that is sound with respect to *sets of sets*: We generate the Galois connection, $\mathcal{P}_\downarrow(\mathcal{P}(C))\langle\alpha_{\rho_{\bar{\mathcal{P}}_L(b)}},\gamma_{\rho_{\bar{\mathcal{P}}_L(b)}}\rangle\mathcal{P}_L(A)$, and for $R : C \to \mathcal{P}(C)$, we generate $R^\sharp_{best} : A \to \mathcal{P}_L(A)$,

$$R^\sharp_{best} = \alpha_{\rho_{\bar{\mathcal{P}}_L(b)}} \circ ext_{\bar{b}}(\{\!\!| \cdot |\!\!\}_{\mathcal{P}_\downarrow(\mathcal{P}(C))} \circ R) \circ \gamma_{\rho_{\bar{b}}}$$

where $ext_{\bar{b}}(\{\!\!|\cdot|\!\!\}_{\mathcal{P}_\downarrow(\mathcal{P}(C))} \circ R)(S) = \downarrow\{R(c) \mid c \in S\}$, and $\alpha_{\rho_{\bar{\mathcal{P}}_L(b)}}(\bar{S}) = \sqcap\{T \mid \text{for all } S \in \bar{S}, S\,\rho_{\mathcal{P}_L(b)}\,T\}$. That is, $ext_{\bar{b}}(\{\!\!| \cdot |\!\!\}_{\mathcal{P}_\downarrow(\mathcal{P}(C))} \circ R)$ maps a set of arguments to the set of R-successor sets, and $\alpha_{\rho_{\bar{\mathcal{P}}_L(b)}}$ produces the smallest abstract set that over-approximates each of the successor sets. We have $R\,\rho_{\bar{b}\to\bar{\mathcal{P}}_L(b)}\,R^\sharp_{best}$, and $R^\sharp_{best}$ equals the definition seen earlier.

This development is notational overkill, but there is an important point: *Simulation equivalence is preserved when a concrete transition function is lifted to a function that maps a set of arguments to a set of sets of answers:*

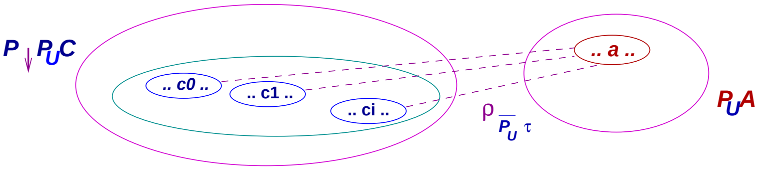
Theorem 16. *$R \lhd_\rho R^\sharp$ iff $R\,\rho_{b\to\mathcal{P}_L(b)}\,R^\sharp$ iff $ext_{\bar{b}}(R)\,\rho_{\bar{b}\to\mathcal{P}_L(b)}\,R^\sharp$ iff $ext_{\bar{b}}(\{\!|\cdot|\!\}_{\bar{\mathcal{P}}_L(b)}\circ R)\,\rho_{\bar{b}\to\bar{\mathcal{P}}_L(b)}\,R^\sharp$.*

This idea will prove crucial when working with under-approximations.

6.1 Synthesizing a most-precise dual simulation

There is a good use for $\rho_{\mathcal{P}_U(\tau)}$: defining a *sound, over-approximation analysis of under-approximations.*

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



We can readily construct $\rho_{\bar{\mathcal{P}}_U(\tau)}$:

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

The resulting Galois connection, $\mathcal{P}_\downarrow(\mathcal{P}_U(C))\langle\alpha_{\rho_{\bar{\mathcal{P}}_U(\tau)}}, \gamma_{\rho_{\bar{\mathcal{P}}_U(\tau)}}\rangle\mathcal{P}_U(A)$, is

$$\gamma_{\rho_{\bar{\mathcal{P}}_U(\tau)}}T = \{S \mid S\,\rho_{\mathcal{P}_U(\tau)}\,T\}$$
$$\alpha_{\rho_{\bar{\mathcal{P}}_U(\tau)}}\bar{S} = \sqcap\{T \in \mathcal{P}_U(A) \mid \text{ for all } S \in \bar{S}, S\,\rho_{\mathcal{P}_U(\tau)}\,T\}$$

Figure 2 presents an example.

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, underapproximating abstract transition relation, $R_0^\flat \subseteq A \times A$ is

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

where $R^{\forall\exists}(M,N)$ *holds iff for all $m \in M$, there exists $n \in N$ such that mRn.* Recoded as a function and simplified, this reads

$$R_0^\flat(a) = \{\alpha(Y) \mid Y \in min\{S' \mid \text{for all } s \in \gamma(a), R(s) \cap S' \neq \{\}\}\}$$

Our machinery gives us the same result: We generate the Galois connection, $\mathcal{P}_\downarrow((\mathcal{P}(C)^{op}))\langle\alpha_{\rho_{\bar{\mathcal{P}}_U(b)}}, \gamma_{\rho_{\bar{\mathcal{P}}_U(b)}}\rangle\mathcal{P}_\uparrow(A)$. Note that C is a set, so $\mathcal{P}(C)^{op}$ is an upper powerset. For transition function, $R : C \to \mathcal{P}(C)$, we generate this most precise, sound under-approximating abstract transition function, $R_{best}^\flat : A \to \mathcal{P}_\uparrow(A)$,

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

where $\{\!|\cdot|\!\}\circ R^{op} : C \rightarrow \mathcal{P}_\downarrow(\mathcal{P}(C)^{op})$ is $(\{\!|\cdot|\!\}\circ R^{op})(c) =\uparrow R(c) = R(c)$, and $\mathit{ext}(\{\!|\cdot|\!\}\circ R^{op}) : \mathcal{P}(C) \rightarrow \mathcal{P}_\downarrow(\mathcal{P}(C)^{op})$ is $\mathit{ext}(\{\!|\cdot|\!\}\circ R^{op})(S) =\downarrow_{\mathcal{P}(C)^{op}} \{R(c) \mid c \in S\} = \{S \supseteq R(c) \mid c \in S\}$, 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, $\mathit{ext}(\{\!|\cdot|\!\}\circ R^{op})$ maps a set of arguments to the set of sets of R-successors, and $\alpha_{\bar{\rho}_{\mathcal{P}_U(b)}}$ produces the largest abstract set that under-approximates each successor set $R(c)$, for $c \in \gamma_{\bar{\rho}_b}(a)$. We simplify and obtain

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

which is provably equal to Dams's definition.[12]

Finally, dual simulation lifts to sets of arguments:

Theorem 17. $R^\flat \lhd_{\rho^{-1}} R$ *iff* $R\,\rho_{b\rightarrow\mathcal{P}_U(b)}\,R^\flat$ *iff* $\mathit{ext}(\{\!|\cdot|\!\}\circ R^{op})\,\rho_{\bar{b}\rightarrow\bar{\mathcal{P}}_U(b)}\,R^\flat$.

It is a good exercise to attempt to define a Galois connection from a $\rho_{\mathcal{P}_U(b)}$; the result is usually degenerate because LUB-closure is over-constraining.[13]

7 Validation and refutation logics

Hennessey and Milner proved that $\Box\Diamond$-propositions (*Hennessey-Milner logic*) characterize transition relations up to bisimilarity [17]. Loiseaux, et al. [22], proved that all $\Box$-properties true of an over-approximating transition relation are preserved in the corresponding concrete transition relation and that when one over-approximating transition relation is more precise than another, then the first preserves all the $\Box$-properties of the second. Dams extended this result to under-approximations and $\Diamond$-properties and proved that his definitions of $R^\sharp_{best}$ and $R^\flat_{best}$ possess the most $\Box\Diamond$-propositions of any sound, mixed transition system.

In this section, we manufacture Hennessey-Milner logic from our family of logical relations (cf. [2]) and obtain the above results as corollaries of Galois-connection theory. Recall that these are the typings of the logical relations,

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

where $\bar{\tau}$ is an instance of $\mathcal{P}_L(\tau)$. For each of the first four typings, we define a corresponding assertion form, producing this assertion language,

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

and the following semantics of typed judgements (let D_τ be either C_τ or A_τ):

$d \models_b p$ *is given, for* $d \in D_b$
$d \models_{\tau_1\rightarrow\tau_2} f.\phi$ *if* $f(d) \models_{\tau_2} \phi$, *for* $d \in D_{\tau_1}$ *and* $f \in D_{\tau_1\rightarrow\tau_2}$
$S \models_{\mathcal{P}_L(\tau)} \forall\phi$ *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* $S \in D_{\mathcal{P}_U(\tau)}$

[12] $R^\flat_0(a)$ belongs to and is $\sqsubseteq$ all elements in $R^\flat_{best}(a)$.

[13] Consider Figure 2 and $\rho_{\mathcal{P}_U(\mathit{Parity})} \subseteq \mathcal{P}(\mathit{Nat})^{op} \times \mathcal{P}_\uparrow(\mathit{Parity})$: What is the least set of natural numbers that "witnesses" $\{\mathit{even}, \mathit{any}\}$? $\{0\}$? $\{2\}$? LUB-closure fails.

Since $\bar{\tau}$ is an instance of $\mathcal{P}_L(\tau)$, we define its judgements for abstract values as

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

and for concrete values as

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

We might abbreviate $d \models_{\tau \to \mathcal{P}_L(\tau)} R.\forall\phi$ by $d \models \forall R\phi$ (as in *description logic* [3]) or by $[R]\phi$ (*Hennessey-Milner logic* [17]) or by $\Box\phi$ when the system studied has only one transition relation, $R \subseteq D_\tau \times D_\tau$ (*CTL* [7]). This hides the reasoning on sets. Similarly, $d \models_{\tau \to \mathcal{P}_U(\tau)} R.\exists\phi$ can be abbreviated by $d \models \exists R\phi$ or $\langle R\rangle\phi$ or $\Diamond\phi$.

The judgements for $\forall\phi$ and $\exists\phi$ employ $R^\sharp$ and $R^\flat$, respectively, to validate the assertions, motivating Dams's mixed transition systems.[14]

7.1 Soundness of judgements

Assume for all types, τ, that the logical relations, $\rho_\tau \subseteq C_\tau \times A_\tau$, are defined. Assume also, for all function symbols, f, typed $\tau_1 \to \tau_2$, that there are interpretations $f : C_{\tau_1} \to C_{\tau_2}$, and $f^\sharp : A_{\tau_1} \to A_{\tau_2}$, such that $f\, \rho_{\tau_1 \to \tau_2}\, f^\sharp$. (Functions f and $f^\sharp$ are used in the semantics of $\models_{\tau_1 \to \tau_2} f.\phi$.)

Definition 18. *Judgement form $\models_{\tau'} \phi$ is* sound *iff for all $c \in C_\tau$, $a \in A_\tau$, ($a \models_{\tau'} \phi$ holds true and $c\, \rho_\tau\, a$) imply that $c \models_{\tau'} \phi$ holds true.*[15]

Assume that $\models_b p$ is sound for the choice of $\rho_b \subseteq C_b \times A_b$.

Theorem 19. *For all types, τ, all judgement forms, $\models_\tau \phi$, are sound.*

The proof is an easy induction on the structure of τ.

We can add the logical connectives,

$$\begin{array}{l} d \models_\tau \phi_1 \wedge \phi_2 \text{ if } d \models_\tau \phi_1 \text{ and } d \models_\tau \phi_2 \\ d \models_\tau \phi_1 \vee \phi_2 \text{ if } d \models_\tau \phi_1 \text{ or } d \models_\tau \phi_2 \end{array}$$

and prove these sound, but we will require a dual logic, a *refutation logic*, to define a sound semantics for $\neg\phi$; we do so momentarily.

7.2 Best precision of judgements

Say that a judgement form, $\models_{\tau'} \phi$, is *monotone* if $a \models_{\tau'} \phi$ and $a' \sqsubseteq_\tau a$ imply $a' \models_{\tau'} \phi$, for all $a, a' \in A_\tau$.[16] We assume that all base-type judgements, $\models_b p_b$, are monotone, and from this it follows that all judgement forms are monotone. As a consequence, we have immediately Dams's best-precision result:

Theorem 20. *For Galois connection, $\mathcal{P}(C)\langle\alpha, \gamma\rangle A$, and every $R : C \to \mathcal{P}(C)$, $R^\sharp_{best} : A \to \mathcal{P}_L(A)$ and $R^\flat_{best} : A \to \mathcal{P}_U(A)$ soundly prove the most typed judgements, $a \models_\tau \phi$, for all $a \in A$ and choices of $\mathcal{P}_L(A)$ and $\mathcal{P}_U(A)$.*

[14] For set, C_τ, $\mathcal{P}(C_\tau)$ is a strongly lower powerset and $\mathcal{P}(C_\tau)^{op}$ is an upper powerset, so we can readily validate $\forall\phi$ and $\exists\phi$-properties on concrete sets, also.

[15] The judgement form, $\models_{\tau_1 \to \tau_2} f.\phi$, shows that τ' need not be τ.

[16] The intuition is that $\gamma_{\rho_\tau}(a') \subseteq \gamma_{\rho_\tau}(a) \subseteq [\![\phi]\!] \subseteq C_\tau$.

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

For $c \in C$, we *define* $c \models_\tau \neg\phi$ *iff* $c \not\models_\tau \phi$.

The logic in Section 7 validates properties, so we might have also a logic that *refutes* them: Read $a \models^{\neg pos}_{\tau'} \phi$ as "it is not possible that any value modelled by $a \in A_\tau$ has property ϕ."

$$
\begin{array}{l}
a \models^{\neg pos}_{b} p \;\; \textit{is given, for } a \in A_b \\
a \models^{\neg pos}_{\tau_1 \to \tau_2} f.\phi \;\; \textit{if } f^\sharp(a) \models^{\neg pos}_{\tau_2} \phi, \textit{ for } a \in A_{\tau_1}, f^\sharp \in A_{\tau_1 \to \tau_2} \\
T \models^{\neg pos}_{\mathcal{P}_U(\tau)} \forall\phi \;\; \textit{if exists } a \tilde{\in} T, a \models^{\neg pos}_{\tau} \phi, \textit{ for } T \in A_{\mathcal{P}_U(\tau)} \\
T \models^{\neg pos}_{\mathcal{P}_L(\tau)} \exists\phi \;\; \textit{if for all } a \tilde{\in} T, a \models^{\neg pos}_{\tau} \phi, \textit{ for } T \in A_{\mathcal{P}_L(\tau)} \\
a \models^{\neg pos}_{\overline{\tau}} \phi \;\; \textit{if } a \models^{\neg pos}_{\tau} \phi, \textit{ for } a \in A_\tau
\end{array}
$$

In the refutation logic, the roles of $\mathcal{P}_L(\tau)$ and $\mathcal{P}_U(\tau)$ are exchanged.

Definition 21. $\models^{\neg pos}_{\tau'} \phi$ *is* sound *iff for all $c \in C_\tau$, $a \in A$, $c\,\rho_\tau\,a$ and $a \models^{\neg pos}_{\tau'} \phi$ imply $c \not\models_{\tau'} \phi$.*

Proposition 22. *For all types, τ, $\models^{\neg pos}_{\tau} \phi$ are sound and monotone, assuming that the base-type judgements, $\models^{\neg pos}_{b} p_b$, are.*[17]

Corollary 23. *The judgement definitions,*
$a \models_\tau \neg\phi$ if $a \models^{\neg pos}_{\tau} \phi$
$a \models^{\neg pos}_{\tau} \neg\phi$ if $a \models_\tau \phi$
are both sound and monotone.

The Sagiv-Reps-Wilhelm TVLA system simultaneously calculates validation and refutation logics[27]. Indeed, we might *combine* $\rho_{\mathcal{P}_L(\tau)}$ and $\rho_{\mathcal{P}_U(\tau)}$ into $\rho_{P_\tau} \subseteq \mathcal{P}(C) \times (\mathcal{P}_L(A) \times \mathcal{P}_U(A))$. This motivates sandwich- and mixed-powerdomains in a theory of over-under-approximation of sets [5, 13, 16, 18, 19].

8 Related work

In addition to Dams's work [10, 11], three other lines of research deserve mention: **Loiseaux, et al. [22]** showed an equivalence between simulations and Galois connections: For *sets* C and A, and $\rho \subseteq C \times A$, they note that
$\mathcal{P}(C)\langle post[\rho], \tilde{pre}[\rho]\rangle\mathcal{P}(A)$ is always a Galois connection.[18]

For $R \subseteq C \times C$ and $R^\sharp \subseteq A \times A$, simulation is equivalently defined as R *is ρ-simulated by $R^\sharp$ iff* $R^{-1} \cdot \rho \subseteq \rho \cdot (R^\sharp)^{-1}$ Treating R^{-1} and $(R^\sharp)^{-1}$ as functions, we can define Galois-connection soundness as

$$
\begin{array}{c}
(R^\sharp)^{-1} \textit{ is a sound over-approximation for } R^{-1} \textit{ with respect to } \gamma \textit{ iff} \\
pre[R] \circ \gamma \sqsubseteq_{\mathcal{P}(A) \to \mathcal{P}(C)} \gamma \circ pre[R^\sharp]
\end{array}
$$

[17] The intuition is that $a \models^{\neg pos}_{\tau'} \phi$ implies $\gamma_{\rho_\tau}(a) \cap [\![\phi]\!] = \{\}$.

[18] $\tilde{pre}[\rho] = \lambda T.\{c \mid \{a \mid c\,\rho\,a\} \subseteq T\}$ is ρ "reduced" to an under-approximation function, and $post[\rho] = \lambda S.\{a \mid \text{ exists } c \in S, c\,\rho\,a\}$. A's partial ordering, if any, is forgotten.

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

1. R is ρ-simulated by $R^\sharp$ iff $(R^\sharp)^{-1}$ is sound for R^{-1} w.r.t. $\widetilde{pre}[\rho]$.
2. $a \models \phi \in ACTL$ [7] implies $c \models \phi$, for $c \, \rho \, a$.

Backhouse and Backhouse [4] saw that Galois connections can be characterized within relational algebra, and they reformulated key results of Abramsky [1]: $\rho \subseteq C \times A$ is a *pair algebra* iff there exist $\alpha : C \to A$ and $\gamma : A \to C$ such that $\{(c, a) \mid \alpha c \sqsubseteq_A a\} = \rho = \{(c, a) \mid c \sqsubseteq_C \gamma a\}$.

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

Ranzato and Tapparo [26] studied the completion of upper closure maps, $\mu : \mathcal{P}(C) \to \mathcal{P}(C)$.[19] Given a logic, $\mathcal{L}$, of form, $\phi ::= op_i(\phi_j)_{0<j<|op_i|}$, its semantics, $[\![\cdot]\!] \subseteq \mathcal{P}(C)$, has format

$$[\![op_i(\phi_j)]\!] = \mathbf{f_i}([\![\phi_j]\!])_{0<j<|op_i|}$$

where each $\mathbf{f_i} : \mathcal{P}(C)^{|op_i|} \to \mathcal{P}(C)$ gives the semantics of connector op_i. The abstract semantics has form, $[\![op_i(\phi_j)]\!]^\mu = (\mu \circ \mathbf{f_i})([\![\phi_j]\!]^\mu)$, and $[\![\phi]\!]^\mu \in \mu[\mathcal{P}(C)]$.

Upper closure μ is *$\mathcal{L}$-preserving* if, for all $S \subseteq C$, $\mu S \subseteq [\![\phi]\!]^\mu$ *implies* $S \subseteq [\![\phi]\!]$, and it is *$\mathcal{L}$-strongly preserving* if the *implies* is replaced by *iff.*

Given an $\mathcal{L}$-preserving μ, Ranzato and Tapparo apply the domain-completion technique of Giacobazzi and Quintarelli [12] to complete μ to its coarsest, strongly preserving form: $\quad complete(\mu) = gfp(\lambda\rho.\mu \sqcap \mathcal{M}(R_{\{\mathbf{f_i}\}}(\rho)))$,
where $\sqcap$ operates in the complete lattice of upper closures, $\mathcal{M}$ is the Moore completion, and $R_F(\mu) = \{f(\bar{x}) \mid f \in F, \bar{x} \in \mu[\mathcal{P}(C)]^{|f|}\}$ adds the image points of the logical operations, $\mathbf{f_i}$, to the domain.

This technique can be applied to the present paper to generate strongly preserving, over- and under-approximating Galois connections.

Acknowledgments

Michael Huth and Radha Jagadeesen provided valuable advice within earlier collaborations. Radhia Cousot provided a supportive environment at École Polytechnique. Tino Cortesi, Patrick Cousot, Dennis Dams, and the referees made useful comments.

References

1. S. Abramsky. Abstract interpretation, logical relations, and Kan extensions. *J. Logic and Computation*, 1:5–41, 1990.

[19] An upper closure map, $\mu : \mathcal{P}(C) \to \mathcal{P}(C)$, is monotone, extensive, and idempotent, and induces the Galois connection, $\mathcal{P}(C)\langle \mu, id \rangle \mu[\mathcal{P}(C)]$.

2. S. Abramsky. Domain theory in logical form. *Ann.Pure Appl.Logic*, 51:1–77, 1991.
3. F. Baader, et al. *The Description Logic Handbook.* Cambridge Univ. Press, 2003.
4. K. Backhouse and R. Backhouse. Galois connections and logical relations. In *Mathematics of Program Construction*, LNCS 2386. Springer Verlag, 2002.
5. P. Buneman, S. Davidson, and A. Watters. A semantics for complex objects and approximate queries. In *7th ACM Symp. Principles of Database Systems*, 1988.
6. M. Ciocoiu. *Ontology-based translation.* PhD thesis, University of Maryland, 2001.
7. E.M. Clarke, O. Grumberg, and D.A. Peled. *Model Checking.* MIT Press, 2000.
8. P. Cousot and R. Cousot. Abstract interpretation frameworks. *J. Logic and Computation*, 2:511–547, 1992.
9. P. Cousot and R. Cousot. Higher-order abstract interpretation. In *Proceedings IEEE Int. Conf. Computer Lang.*, 1994.
10. D. Dams. *Abstract interpretation and partition refinement for model checking.* PhD thesis, Technische Universiteit Eindhoven, The Netherlands, 1996.
11. D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. Prog. Lang. Systems*, 19:253–291, 1997.
12. R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples, and refinements in abstract model checking. In *Static Analysis Symposium*, LNCS 2126, pages 356–373. Springer Verlag, 2001.
13. C. Gunter. The mixed power domain. *Theoretical Comp. Sci.*, 103:311–334, 1992.
14. J. Hartmanis and R.E. Stearns. Pair algebras and their application to automata theory. *J. Information and Control*, 7:485–507, 1964.
15. R. Heckmann. *Power domain constructions.* PhD thesis, Univ. Saarbrücken, 1990.
16. R. Heckmann. Set domains. In *Proc. European Symp. Programming*, LNCS, pages 177–196. Springer Verlag, 1990.
17. M.C.B. Hennessy and Robin Milner. Algebraic laws for non-determinism and concurrency. *JACM*, 32:137–161, 1985.
18. M. Huth, R. Jagadeesan, and D.A. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In *Proc. European Symp. Programming*, LNCS, pages 155–169. Springer Verlag, 2001.
19. M. Huth, R. Jagadeesan, and D.A. Schmidt. A domain equation for refinement of partial systems. *Mathematical Structures in Computer Science*, 2004. In press.
20. D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.
21. K.G. Larsen. Modal Specifications. In *Automatic Verification Methods for Finite State Systems*, LNCS 407, pages 232–246. Springer Verlag, 1989.
22. C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property preserving abstractions for verification of concurrent systems. *Formal Methods in System Design*, 6:1–36, 1995.
23. A. Mycroft and N.D. Jones. A relational framework for abstract interpretation. In *Programs as Data Objects*, LNCS 217, pages 156–171. Springer Verlag, 1985.
24. F. Nielson. Two-level semantics and abstract interpretation. *Theoretical Comp. Sci.*, 69:117–242, 1989.
25. G. Plotkin. Domains. Lecture notes, Univ. Pisa/Edinburgh, 1983.
26. F. Ranzato and F. Tapparo. Strong preservation as completeness in abstract interpretation. In *Proc. European Symp. Programming*, LNCS 2986, pages 18–32. Springer Verlag, 2004.
27. M. Sagiv, T. Reps, and R. Wilhelm. Parametric shape analysis via 3-valued logic. In *Proceedings 28th ACM POPL*, 1999.
28. D.A. Schmidt. Structure-preserving binary relations for program abstraction. In *The Essence of Computation*, LNCS 2566, pages 246–266. Springer Verlag, 2002.